Technical Report 06-01
July 2006

Development and Application of Skill Standards for Security Practitioners

Henry K. Simpson
Northrop Grumman Technical Services

Lynn F. Fischer
Defense Personnel Security Research Center

John D. Tippit
The Tippit Group

Alissa Hayes
Northrop Grumman Technical Services

Approved for Public Distribution: Distribution Unlimited
Defense Personnel Security Research Center

Technical Report 06-01 **July 2006**

Development and Application of Skill Standards for Security Practitioners

Henry K. Simpson, Northrop Grumman Technical Services
Lynn F. Fischer, Defense Personnel Security Research Center
John D. Tippit, The Tippit Group
Alissa Hayes, Northrop Grumman Technical Services

Released By – James A. Riedel

BACKGROUND

Federal agencies, government contractors, and the military services require well-trained and competent security personnel to ensure the effective administration of their security programs. The Joint Security Training Consortium (JSTC) requested the Defense Personnel Security Research Center to conduct research and development work to improve the training and professional development of the security workforce. The work described in the present report was driven by a JSTC tasking to develop skill standards for security practitioners in seven different security disciplines: security management, security investigations, and communications, physical, information, personnel, and information systems security. Skill standards define competent job performance and the underlying knowledge and skills that competent workers must possess. They are powerful tools with many different applications for training and career development.

HIGHLIGHTS

This report describes how the skill standards for security practitioners were produced and presents the skill standards taxonomies for each of the seven security disciplines as they were developed by subject-matter experts. The report also provides guidance to help end-users put the standards to work in practical applications including training development, training assessment, job performance evaluation, job definition, and professional certification.

Defense Personnel Security Research Center
99 Pacific Street, Suite 455-E
Monterey, CA 93940-2497

REPORT DOCUMENTATION PAGE

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE: 01-07-2006

2. REPORT TYPE
Technical Report 06-01

3. DATES COVERED
August 2005 - July 2006

4. Development and Application of Skill Standards for Security Practitioners

5a. CONTRACT NUMBER:

5b. GRANT NUMBER:

5c. PROGRAM ELEMENT NUMBER:

6. AUTHOR(S)
Henry K. Simpson, Lynn F. Fischer, John D. Tippit, Alissa Hayes

5d. PROJECT NUMBER:

5e. TASK NUMBER:

5f. WORK UNIT NUMBER:

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Defense Personnel Security Research Center
99 Pacific Street, Suite 455-E
Monterey, CA 93940-2497

8. PERFORMING ORGANIZATION REPORT NUMBER
PERSEREC: Technical Report 06-01

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Defense Personnel Security Research Center
99 Pacific Street, Suite 455-E
Monterey, CA 93940-2497

10. SPONSORING/MONITOR’S ACRONYM(S):
PERSEREC

11. SPONSORING/MONITOR’S REPORT NUMBER(S):

12. DISTRIBUTION/AVAILABILITY STATEMENT: Distribution Unlimited

13. SUPPLEMENTARY NOTES:
Appended to this report is a lengthy taxonomy containing detailed skill standards for each of seven core security disciplines.

14. ABSTRACT:
The work covered in this report was driven by a Joint Security Training Consortium tasking to develop skill standards for security practitioners in seven different security disciplines: physical security, information security, personnel security, security investigations, security management, communications security, and information systems security. These skill standards apply to all Federal agencies and define competent job performance and the underlying knowledge and skills that competent workers must possess. This report describes how the skill standards were developed and presents the skill standards for each of the seven security disciplines. It also presents guidance to help end-users put the standards to work in five practical applications: Training Definition, Training Assessment, Performance Evaluation, Job Definition, and Professional Certification. The skill standards and application guidance in this report are intended for use as tools rather than as prescriptions, and readers are encouraged to modify them as needed based on their particular requirements.

15. SUBJECT TERMS:
Skill Standards, Security, Security Disciplines, Job Analysis, Information Security, Personnel Security, Communications Security, Investigations, Security Management, Physical Security, Information Systems Security

16. SECURITY CLASSIFICATION OF:
UNCLASSIFIED

a. REPORT:
UNCLASSIFIED

b. ABSTRACT:
UNCLASSIFIED

c. THIS PAGE:
UNCLASSIFIED

17. LIMITATION OF ABSTRACT:
None.

18. NUMBER OF PAGES:
68

19a. NAME OF REPONSIBLE PERSON: James A. Riedel, Director

19b. TELEPHONE NUMBER (Include area code): 831-657-3000

PREFACE

In response to a longstanding and well-documented need, the Joint Security Training Consortium (JSTC) requested the Defense Personnel Security Research Center (PERSEREC) to conduct research and development to improve the training and professional development of security personnel. Over the past 3 years, PERSEREC has conducted several projects for JSTC relating to the training and professional development of security practitioners. These include scoping the landscape of security training issuances, developing a baseline definition of the security profession, investigating professional development and certification programs for security job incumbents, and developing training policy for security practitioners.

The work covered in the present report was driven by a JSTC tasking to develop skill standards for security practitioners in seven different security disciplines: physical security, information security, personnel security, security investigations, security management, communications security, and information systems security. Skill standards define competent job performance and the underlying knowledge and skills that competent workers must possess. Skill standards are powerful tools and have many applications, including training definition, training assessment, job performance evaluation, job definition, and certification. They can help the trainer to develop and assess training, the supervisor to rate or test worker performance, or the employer to write job descriptions or design certification programs.

This report describes how the skill standards were developed and presents the skill standards for each of the seven security disciplines. It also presents guidance to help end-users put the standards to work in practical applications. The skill standards and application guidance in this report are intended for use as tools rather than as prescriptions, and readers are encouraged to modify them as needed based on their particular requirements.

James A. Riedel
Director

PREFACE

ACKNOWLEDGMENTS

The authors greatly appreciate the contributions of the many individuals who participated in the work described in this report. This work derives directly from the vision of Geoff Watson, formerly the director of the Joint Security Training Consortium, to create a complete set of skill standards in the core security disciplines as practiced by the federal workforce. The standards were developed based on a method used by the National Skill Standards Board. Dr. Joselito Lualhati, formerly of the NSSB and currently the Research and Development Director at Global Skills Exchange, participated in all workshops, facilitated sessions, obtained subject-matter expert ratings, and ensured that the final products conform to National Skill Standards Board guidelines and conventions.

A total of 49 subject-matter experts participated in workshops (names and organizational affiliations are given in Exhibit B-2 in Appendix B). We thank those experts for sharing their expertise with us for the benefit of the security community. We are particularly grateful to Richard Williams, formerly the Director of Security Programs for OSD, who participated in all seven workshops, provided continuity, and contributed his sound judgment, leadership, and good humor. Federal employees who participated were funded by their agencies and we are indebted to those agencies for their support. The agencies include the Defense Security Service, Department of State, Defense Advanced Research Projects Agency, Defense Threat Reduction Agency, Air Force Office of Special Investigations, Federal Aviation Agency, USAF Declassification Office, The Joint Chiefs of Staff, Information Security Oversight Office, Naval Criminal Investigative Service, National Security Agency, Department of the Army, Office of the Secretary of Defense, and the Federal Bureau of Investigation.

ACKNOWLEDGMENTS

EXECUTIVE SUMMARY

BACKGROUND

There is a great need for government, government contractors, and the military services to field well-trained and competent security personnel. Adequate training is essential for competent performance. Despite this relationship, several national-level security reviews and audits performed in the last decade have criticized the training and performance of security personnel. The Joint Security Training Consortium (JSTC) requested the Defense Personnel Security Research Center (PERSEREC) to conduct research and development work to improve the training and professional development of security personnel. The work covered in the present report was driven by a JSTC tasking to develop skill standards for security practitioners, a logical extension of PERSEREC's earlier project to develop a baseline definition of the security profession in terms of draft taxonomies describing the work performed by security practitioners in seven security disciplines: physical security, information security, personnel security, security investigations, security management, communications security, and information systems security. The seven taxonomies were intended to be the first step in developing an authoritative description of what security personnel do on the job.

Skill standards describe competent job performance and the underlying knowledge and skills (K&S) that competent workers must possess. The taxonomies were the starting point for the current work and, since the skill standards would be based on them, there was a requirement to vet the taxonomies before developing the standards. The National Skill Standards Board (NSSB) has documented and successfully implemented a formal method to develop skill standards for industrial occupational groups of workers who perform similar jobs and with workforce populations much larger than the entire federal and contractor security workforce. The method is time- and labor-intensive and had to be rescaled for the smaller security workforce and the greater diversity of work performed by security personnel. Skill standards have many applications, but the study focused on five of them: training definition, training assessment, job performance evaluation, job definition, and certification. The standards define competent job performance and the underlying K&S, but applying them to define training, evaluate job performance, and in other applications is a separate matter. Each of the applications generated a requirement to develop guidance to help the end-users of the standards to perform their application.

OBJECTIVES

The objectives of this project were as follows:

- Vet the taxonomies for the seven security disciplines in the baseline definition of security profession

- Develop skill standards for the seven security disciplines
- Document the method used to develop skill standards
- Develop guidance to help end-users apply the skill standards to support training definition, training assessment, job performance evaluation, job definition, and certification.

METHOD

The method consists of the following steps:

- Conduct Job Analysis. A job analysis was conducted to develop taxonomies that describe the work performed by security professionals based on a review of security job-related documentation, subject-matter expertise, analyses, and recommendations from subject-matter experts (SME).
- Conduct SME Workshops. Workshops were conducted to vet the taxonomies and obtain input from SMEs that would enable development of skill standards. Separate workshops were conducted for each of the seven security disciplines. SMEs were designated by senior security personnel in DoD agencies and departments, and PERSEREC subcontracted several retired security personnel to participate. SMEs completed pre-workshop tasks to prepare themselves. The workshops were conducted over three workdays and attended by SMEs, facilitators, and an NSSB job analyst. During each workshop, SMEs individually presented recommended changes to the taxonomy to their peers, reviewed source documents to determine if their information content should be reflected in the taxonomy, and participated in a working session with an NSSB job analyst to elicit K&S requirements and provide ratings.
- Derive Skill Standards. Following the workshop, the NSSB job analyst integrated workshop products into a set of skill standards, SMEs reviewed them, and a final set of standards was generated.

Skill Standards

A separate set of skill standards was developed for each of the seven security disciplines. In overview, each set of standards describes (1) what workers do on the job and (2) the K&S needed to perform successfully as entry-level, journeyman, and senior security professionals. More specifically, each set of skill standards consists of the following elements:

- Work Taxonomy. A three-level taxonomy describes what workers do on the job in terms of Critical Work Functions (major responsibilities), Key Activities (major duties or tasks), and Performance Indicators (information used to judge competent performance).
- Key Activity Knowledge and Performance Level Expectations by Seniority. These are SME estimates of the knowledge and performance levels required to perform each Key Activity at entry, journeyman, and senior levels.

- Academic and Employability K&S Work Relevance and Importance by Seniority. Academic K&S are associated with the academic disciplines of reading, writing, mathematics, and science. Employability K&S are general workplace K&S such as such as teamwork, decision making, and problem solving. This element consists of SME estimates of work relevance and importance at entry, journeyman, and senior levels.
- Occupational and Technical K&S Work Relevance and Complexity by Seniority. Occupational and Technical K&S apply to the specific type of work. This element consists of SME estimates of work relevance and the complexity levels workers must be able to handle at entry, journeyman, and senior levels.

Skill Standards Application Guidance

Application guidance was developed to assist end-users of skill standards to use them in five practical applications: Training Definition (the process of designing training), Training Assessment (assessing training that already exists), Performance Evaluation (evaluating worker job performance), Job Definition (defining a particular type of job), and Certification (determining whether or not a worker is able to meet criteria and standards required at a particular seniority level). Guidance describes each of the five applications, discusses several considerations that apply to all of them, and then describes and illustrates each application in more detail.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF TABLES IN APPENDICES

LIST OF FIGURES IN APPENDICES

LIST OF WORKSHOP EXHIBITS IN APPENDICES

LIST OF SKILL STANDARDS IN APPENDICES

INTRODUCTION

OVERVIEW

This report describes research and development work leading up to the development of skill standards for security practitioners, presents the standards, and provides guidance for using them in several different applications. This is a long report and readers may find it beneficial to focus their reading based on their particular interests. To this end, report content is sketched briefly below:

- *Introduction* describes the research problem, requirements, and potential applications of the skill standards
- *Objectives* lists the project objectives
- *Job Analysis Overview* describes traditional job analysis and the National Skill Standards Board (NSSB) job analysis method
- *Method* describes how the skill standards were developed
- *Skill Standards Overview* describes the structure, content, and format of the skill standards. (This content is duplicated in Appendix C.)
- *Applying the Skill Standards* provides guidance about how to apply the skill standards in training definition, training assessment, performance evaluation, job definition, and certification
- *Skill Standards* (Appendices D-J) presents the skill standards

Readers interested in how the standards were developed should find the entire report useful. Readers interested in applying the standards will probably find *Skill Standards Overview*, *Applying the Skill Standards*, and *Skill Standards* the most useful. Readers interested in developing skill standards of their own will probably find *Job Analysis*, *Method*, *Skill Standards Overview*, and *Skill Standards* the most useful.

THE PROBLEM

There is a great need for government, government contractors, and the military services to field competent security personnel. Adequate training underlies competent performance, but many authoritative reviews and audits have criticized the training and performance of security personnel (e.g., DoD Security Review Commission, 1985; Joint Security Commission, 1994, 1999; General Accounting Office [1994, 1996a, 1996b, 1996c, 1999, 2002a, 2002b]). The problem is widely acknowledged, longstanding, and needs to be addressed.

A recent PERSEREC study of the security profession observed that the defense and intelligence communities have large training infrastructures and share common core training requirements that are poorly defined; that agency training programs are largely independent and conducted in disciplinary stovepipes, resulting in inconsistent training quality, duplication of effort, increased cost, and uneven performance; and that most security training focuses on basic skills and reflects little or no effort to professionalize the workforce (Tippit, Rizzoli, Baker, & Miller, 2002). Tippit et al. characterized security work as a “profession by practice” because it largely lacks an academic foundation and most practitioners enter without formal security training. Security work has few entry barriers, which reduces its credibility as a profession. There is also great variance among security practitioners in terms of their background, training, work responsibilities, and duties. This training picture, they concluded, represents a risk to the successful execution of the security mission.

The Joint Security Training Consortium (JSTC), a jointly coordinated and funded initiative of the DoD and the intelligence community, was established to provide a coordinated, cross-community response to several long-term issues associated with the training and professional development of security personnel. The JSTC requested the Defense Personnel Security Research Center (PERSEREC) to conduct research and development concerning a number of security training issues. These include scoping the landscape of security training issuances (Tippit, Rizzoli, Denk, & Fischer, 2001; Tippit & Rizzoli, 2001, 2003), developing a baseline definition of the security profession (Tippit et al., 2002), investigating professional development and certification programs for security job incumbents (Fischer, 2004; Marshall-Mies & Fischer, 2003; Marshall-Mies, Lupton, & Fischer, 2003; Tippit & Askia, 2002), developing training policy for security practitioners (Simpson, Fischer, Tippit, Rizzoli, & Denk, 2004), and developing skill standards for security practitioners.

THE REQUIREMENTS

PERSEREC work for JSTC has been conducted to improve the training and professional development of security personnel. The work covered in the present report was driven by a JSTC tasking to develop skill standards for security practitioners. The JSTC had established a partnership and contractual relationship with the NSSB to support development of the standards. The NSSB was created as a result of the National Skill Standards Act of 1994, which included a sunset provision that took effect in 2003. While active, the NSSB created a method to develop skill standards that was widely applied in industry and that had significant credibility. Before it was disestablished, the NSSB developed standards for two subsets of the Personnel Security disciplines (Background Investigations and Adjudication). Finding it difficult to enlist the services of agency representatives for several days of intensive effort, the JSTC requested PERSEREC to complete the work that had been started by completing standards for each of the core security disciplines.

This tasking was a logical extension of PERSEREC's work to develop a baseline definition of the security profession (Tippit et al., 2002). That study developed draft taxonomies describing the work performed by security practitioners in seven security disciplines: physical security, information security, personnel security, security investigations, security management, communications security, and information systems security.[1] The seven taxonomies were intended to be the first step in developing an authoritative description of what security personnel do on the job. Tippit et al. (2002) suggested four possible uses for the taxonomies:

1. Build consensus on the architecture of the security profession
2. Develop a common language for the security profession
3. Define the core competencies of security practitioners in support of training
4. Define the expected level of performance at different stages of a security practitioner's career (e.g., novice, journeyman, expert)2

The first two uses describe the security profession itself. The authors offered the taxonomies to the security community as tools and resources to use to define what security practitioners do and to refine the lexicon needed to reach consensus. The third and fourth uses deal with defining training needed and performance expected at different levels of seniority. The taxonomies were published as a baseline product that would require expert vetting.

Vetting the Taxonomies

These baseline taxonomies were developed from a literature review, on-site interviews with security practitioners, analyses[3], and review by security subject-matter experts (SME). They were the starting point for the current work and, since the skill standards would be based on them, there was a requirement to vet the taxonomies before developing the standards.

Developing Skill Standards

The authors of this report use the term *skill standards* in accordance with the usage of the National Skill Standards Board (2000a), which states that skill standards should answer two fundamental questions:

1. What does someone need to do on the job to perform competently?
2. What knowledge and skills will enable them to carry out these responsibilities?

[1] Tippit et al. acknowledged that additional security activities are performed beyond these seven disciplines but regarded these seven as the main ones.

[2] The three-level *novice*, *journeyman*, and *expert* distinction is commonly used in describing personnel workforce career levels. Another common way is *entry level*, *mid level*, and *senior level*.

[3] The specific types of analyses performed are described in the *Method* section.

Both questions relate to the workplace, but the answers have wider application. For example, McCormick (1979), in an authoritative text on job analysis, offers several possible users and nearly two dozen applications of such information (see Table 1). While skill standards have many applications, the current study was conducted to improve the training and professional development of security personnel, and the key applications are training definition, training assessment, job performance evaluation, job definition, and certification.

Skill standards were developed based on a job analysis and a method adapted from that used by the NSSB as documented in several different publications (e.g., National Skill Standards Board, 2000a, 2000b, 2002a, 2002b).

Table 1
Partial Listing of Possible Users and Applications of Skill Standards (from McCormick, 1979)

Users	Applications
Employer	Personnel recruitment
	Personnel selection and placement
	Personnel evaluation
	Job design
	Training and personnel development
	Personnel utilization
	Manpower planning
	Establishment of lines of responsibility
	Establishment of organizational relationships
Government Agencies	Occupational standards, licensing, certification, etc.
	Equal employment opportunity matters
	Public employment service
	Public training and education programs
	Social security matters including unemployment compensation
	Working conditions, safety, etc.
Individuals	Vocational selection
	Vocational preparation
Researchers	Personnel and other behavioral research
	Sociological research
	Demographic (i.e., population) research
	Economic research

Applying the Skill Standards

The applications of particular interest were training definition, training assessment, job performance evaluation, job definition, and certification. The standards define competent job performance and the underlying knowledge and skills (K&S), but applying them to define training, evaluate job performance, and in other applications is a separate matter. Each of the applications generates a requirement to develop guidance to help the end-users of the standards to accomplish the goals.

OBJECTIVES

The objectives of this project were as follows:

- Vet the taxonomies for the seven security disciplines in the baseline definition of security profession
- Develop skill standards for the seven security disciplines
- Document the method used to develop skill standards
- Develop guidance to help end-users apply the skill standards to support training definition, training assessment, job performance evaluation, job definition, and certification

JOB ANALYSIS

The method used to develop skill standards was adapted from that used by the NSSB which, in turn, is a variant of traditional job analysis. The NSSB method defines job dimensions with terminology that is specialized and somewhat at variance with common usage. Hence, to help readers bridge the gap, this section first describes traditional job analysis and then the NSSB job analysis method. *Method* tells how the NSSB method was adapted to the present project.

TRADITIONAL JOB ANALYSIS

The following description is based primarily on McCormick (1979), Brannick and Levine (2002), and Cascio (1991). As noted in the Introduction, job analysis is performed for many different purposes. There is no single way to conduct analysis, but analyses often share certain common features. Some of the basics are discussed below.

Terminology

Job analysis is the process of obtaining information about jobs. The information obtained from analysis is commonly described in hierarchical terms, from highest to lowest levels, as follows:

- Career—sequence of positions, jobs, occupations during a person's working life
- Occupation—group of similar jobs in different organizations/times
- Job family—group of two or more related jobs
- Job—group of related positions
- Duty—segment of work comprised of tasks
- Task—distinct work activity carried out for a distinct purpose
- Element—smallest inseparable unit of work

Each term represents the cluster of terms beneath it. For example, a *duty* consists of its underlying cluster of *tasks*, and each *task* its underlying cluster of *elements*.

The definitions of these terms are general enough that terminology may present problems to job analysts. McCormick quotes Melching and Borcher (1973) on this point:

> While job analysis experts employ concepts such as task, function, responsibility, duty, etc. as though the distinctions among them were both obvious and fixed, this is simply not true....

One common analysis problem is deciding at what level a particular descriptive job term applies, for example, should something be called a "task" or a "duty"? This is often not as obvious as the definitions seem to suggest. Another problem analysts may face is deciding whether the levels are enough or too many. For example, might one fit a “subtask” between element and task? There are no fixed rules for making these decisions. They are based on judgment and are somewhat subjective.

Job analysis shares some terminology with education and training since both need to describe worker K&S. K&S are typically acquired in the schoolhouse and later applied on the job. They may also be acquired on the job. In simple terms, knowledge is what a worker knows, and skill is what the worker is able to do.[4]

It is important to clarify the difference between education and training. Both involve instruction and applied exercises to develop K&S, but differ in terms of their focus on academic versus vocational or professional K&S. Education concerns academic K&S and training vocational or professional K&S.

Types of Job Information

Job analysis information falls into two broad categories:

- Work attributes—what the worker does to perform the job successfully
- Worker attributes—what K&S are required to perform the job

This is an oversimplification, but helpful in thinking about how job analysis information may be structured.

Work attributes may be thought of as the tasks performed on the job. Worker attributes are more complex because they comprise everything the worker brings to the job in terms of prior education, training, work experience, and background. Table 2 is a simple taxonomy that lists three types of K&S, what they are, and where they are likely to be acquired. The K&S are of three types: academic, general workplace, and job-specific technical:

- Academic K&S relate to general literacy and numeracy and are usually acquired in the schoolhouse.
- General workplace K&S are nontechnical K&S essential for effective performance in the workplace and are usually gained in the workplace.
- Job-specific technical K&S are those K&S needed to perform the job-specific technical aspects of the job. Technical K&S do not necessarily require the use of technology.

[4] The U.S. Department of Labor (2004) formally defines *knowledge* as “a body of information applied directly to the performance of a function” and *skill* as “an observable competence to perform a learned psychomotor act”. It adds to this mix the term *ability* as “the attributes required to perform a job [that] are generally demonstrated through qualifying service, education, or training”. The distinction between skill and ability is at best vague and the ability term is not in the job analysis lexicon.

Table 2
A Simple Taxonomy of Worker Attributes

Types of K&S	Description	Where Acquired
Academic	K&S associated with the academic disciplines of reading, writing, mathematics and science	Academic institutions
General workplace	Applied K&S – such as teamwork, decision-making, and problem solving – used to perform effectively across a broad ranges of occupations	Workplace
Job-specific technical	Specific technical K&S needed to perform job	Technical and professional training, workplace

Analysis Objectives

The broad objective of job analysis is to gather, develop, estimate, and describe the types of information discussed above. This objective may be expressed in terms of two subobjectives:

- Define the work attributes of interest in the eventual application, for example, such attributes as job family, jobs, duties, tasks, and task elements
- Define the worker attributes necessary to perform the job successfully in terms of academic, general workplace, and job-specific K&S

The breadth of these objectives will vary with the scope of the analysis. The study of an occupation with many job families, jobs, and a large worker population will need to be broader in scope than a study concerning a smaller-scale occupation.

Obtaining Job Information

Job information may be obtained in many different ways and addresses some or all of the objectives listed above. The ways commonly cited are:

- Review job-related documentation such as training materials, job analyses, job descriptions, operating procedures, policies, records, and reports
- Interview individual job incumbents, supervisors, SMEs and others with job knowledge and experience. Alternatively, conduct group interviews with several personnel
- Observe a job incumbent perform the job in the workplace. The observer may concurrently interview the worker
- Convene panels of SMEs to generate, review, and validate job information
- Perform the job to gain direct experience concerning work attributes
- Conduct a conference to bring together experts to identify, focus, and address job-related issues

- Develop a structured questionnaire and survey job incumbents, supervisors, SMEs and others with job knowledge and experience

Some other ways to obtain information are open-ended questionnaires, critical incidents (examples of good and poor job performance), job incumbent narrative descriptions of work activities, work records, and design information concerning equipment used on the job.

There are no strict rules governing how to obtain job information in a particular analysis. The decision is based on judgment and should consider several factors. Among these are relative cost, available analysis resources, existing job information, access to workers, workforce size, consequences of inadequate job performance, and availability of SMEs.

It is reasonable to start by reviewing job-related documentation, if available, since this is inexpensive and allows the analyst to leverage existing job information and possibly earlier analyses.

Job analysts must understand the job they are analyzing and usually need to work with SMEs and SME panels. It is hard to imagine conducting an analysis without SMEs unless the analyst is already an SME or the job is very simple.

Beyond this, it is difficult to generalize except that the information gathered must capture work and worker attributes fully and accurately. In large workforce studies it is standard practice to conduct many interviews, observe many workers on the job, and gather additional information with questionnaires. “Many” often translates as hundreds or thousands. Critical incident studies are especially important if inadequate performance may have serious negative outcomes affecting, for example, safety or high cost.

NSSB JOB ANALYSIS METHOD

The NSSB job analysis method is a variation of traditional job analysis and much of the earlier description applies directly. The NSSB documented its method in several publications (e.g., National Skill Standards Board, 2000a, 2000b, 2002a, 2002b), and the following description is based on these sources.

Most of the traditional job analysis terminology applies to NSSB job analysis, but nomenclature differs slightly, as shown in Table 3. For example, NSSB names for Duties, Tasks, and Elements are, respectively, Critical Work Functions (CWF), Key Activities (KA), and Performance Indicators (PI). Traditional and NSSB job analyses are equally concerned with work and worker attributes although the labels attached to these categories differ somewhat. Arguably, the NSSB terminology is less transparent than traditional terminology and may be confusing if one does not keep the definitions in mind. Recall that these terms are hierarchical, with each label representing the cluster of elements beneath it, for example, each CWF contains its underlying cluster of KAs, and each KA its underlying cluster of PIs. Note that KAs are what people commonly use to describe a job. CWFs are categories used to group related KAs under a common label. In addition, once a KA is selected, its PIs go with it.

Table 3
Comparative Terminology of Traditional and NSSB Job Analysis

Terminology		NSSB Definition (traditional definition is equivalent)
Traditional	NSSB	
Work Attributes	Work-oriented Component	What the worker does to perform the job successfully
Worker Attributes	Worker-oriented Component	What K&S are required to perform the job
Duties	Critical Work Functions (CWF)	Major responsibilities of work
Tasks	Key Activities (KA)	Major duties or tasks involved in carrying out a critical work function
Elements	Performance Indicators (PI)	Information on how to determine when someone is performing a key activity competently
Academic K&S	Academic K&S	K&S associated with the academic disciplines of reading, writing, mathematics and science
General Workplace K&S	Employability K&S	K&S such as teamwork, decision making, and problem solving that apply across a broad ranges of occupations
Job-Specific Technical K&S	Occupational & Technical K&S (OTKS)	K&S that apply to the specific type of work

The correspondence between duty and CWF or task and KA is straightforward, but it is less obvious how a task element applies as a PI. The NSSB logic seems to be that KA performance can be judged based on whether or not and how well its underlying PIs are performed.

To reiterate a point made in the introduction, the NSSB defines *skill standards* as what must be done on the job to perform competently and the K&S that underpin performance—in other words, the combination of work and worker attributes that emerge from job analysis.

NSSB analysis objectives and ways of obtaining job information all fit within the traditional job analysis framework. Historically, the NSSB method has been used mainly to develop skill standards for industrial occupational groups with large populations of workers who perform similar jobs. For example, an NSSB work and analysis plan for the information and communications technology (ICT) sector lists four industrial occupation fields each comprising one million or more job incumbents (National Skill Standards Board, 2002a). The large workforce size justifies the allocation of considerable resources and effort to obtain and validate job analysis information. *Built to Work: A Common Framework for Skill Standards* (National Skill Standards Board, 2000a) outlines a method that systematically analyzes workplace performance by forming voluntary partnerships in several different organizations; consulting with large numbers of personnel with workplace, subject matter, and job analysis expertise (e.g., managers, trainers, educators, recruiters, human resources staff, job analysts); and validating the results in a large-scale field survey of workers.

The foregoing should give a sense of the scale, level of effort, and resource requirements of the NSSB job analysis process. Fischer (2004) estimated the federal security workforce at approximately 10,000 with perhaps twice that number in the contractor community—a few percent of the size of the ICT population cited above. Moreover, the security workforce is quite diverse in terms of the responsibilities and tasks performed by security practitioners, making it more difficult to conduct a field validation survey. The NSSB method is time- and labor-intensive and had to be rescaled and adapted for application with the much smaller security workforce and the large number of different jobs performed by security personnel working in each discipline. In a nutshell—and as will be apparent in the *Method* section that follows—this was done by consulting with proportionally fewer organizations and security personnel and deferring the field survey to be performed later, if needed, by end-users.[5]

[5] *Applying the Skill Standards* discusses the relative importance of conducting validation surveys for different types of applications under the subsection titled *Cautionary Notes.*

METHODOLOGY

This section describes the steps followed in developing the skill standards. These include developing work taxonomies, adapting the NSSB method, planning and conducting SME workshops, and conducting analyses to develop the skill standards. The method echoes much of the job analysis description in the *Job Analysis Overview* section.

DEVELOP WORK TAXONOMIES

Taxonomies were developed to describe the work performed by security personnel (i.e., what NSSB calls the "work-oriented component") of skill standards. Four SMEs from the Tippit Group compiled the taxonomies from a review of security job-related documentation, their own subject-matter expertise, analyses, and recommendations from SMEs who were interviewed and members of the security community who reviewed their draft taxonomies.

Security Documentation Review

A team of SMEs and analysts gathered and reviewed a variety of security job-related documents while developing their baseline definition of the security profession (Tippit et al., 2002). Their bibliography is shown at Appendix A. In overview, it includes the following types of documents:

- Policy relating to security practice, workforce training, and protection
- Training course descriptions, curricula, training objectives and standards
- Security job documentation such as position descriptions, job manuals, performance standards, and descriptions of professional development programs
- Professional and academic texts relating to security work and careers
- Technical reports and studies concerning security issues, and security workforce composition, size, compensation, and resources
- Governmental and private sector reviews and studies of security programs, processes, and operational structures

Analyses

Analysis focused on federal civilians, federal contractors, and military personnel; on security personnel working at journeyman (mid) level and excluded those working at entry (basic) and senior (expert) level; and on CWF, KA, and PI that are technical (i.e., security-related) versus nontechnical (e.g., management, administrative).

Analysis proceeded in a top-down fashion:

- Determine common security position job titles, concentrations, and specializations. Tippit et al. listed 50, with much redundancy and overlap in terms of responsibilities and tasks performed.
- Develop and apply a screening protocol to cluster titles, concentrations, and specializations to shred out disciplines based on common required skills, knowledge, and abilities. Tippit et al. identified seven basic security disciplines but acknowledged that additional security activities are performed beyond these disciplines.
- Define where the basic security disciplines fit within the larger community of related professions (such as criminal justice/law enforcement, intelligence, counterintelligence, and safety and emergency services). Table 4 illustrates the landscape of disciplines and related professions, and shows how the basic security disciplines fit into the picture.
- Identify the CWFs and KAs in each of the seven disciplines.[6]
- Compare the initial findings with mature examples of both public and private sector definitions of the security profession.
- Develop the taxonomies

Table 4
The Security Profession—The Big Picture
(from Tippit et al., 2001)

CRIMINAL JUSTICE	BASIC SECURITY DISCIPLINES	SAFETY & EMERGENCY SERVICES
JUDICIARY	PHYSICAL SECURITY	EMERGENCY AND DISASTER RESPONSE
CORRECTIONS	PERSONNEL SECURITY	EMERGENCY AND DISASTER PREPAREDNESS
LAW ENFORCEMENT	INFORMATION SECURITY	WORKPLACE SAFETY
KEY LE MISSIONS • MAINTAIN ORDER • PROTECT LIFE & PROPERTY • PREVENT CRIME • ENFORCE LAWS • DETECT & APPREHEND • OFFENDERS • PERFORM OTHER SERVICES	COMMUNICATION SECURITY	SPECIAL HAZARDS RESPONSE
	INFORMATION SYSTEM SECURITY	INTELLIGENCE AND COUNTERINTELLIGENCE
	INVESTIGATIONS	DOMESTIC
	SECURITY MANAGEMENT	FOREIGN

Taxonomy content is structured at five levels from highest (1) to lowest (5):

1. Entire security profession
2. Security disciplines
3. CWFs comprising each discipline
4. KAs comprising each CWF
5. PIs comprising each KA

The foregoing condenses and simplifies what was in fact a somewhat nonlinear, iterative, analytical and judgment-based process that defies easy description. It was

[6] Tippit et al. used somewhat different terminology but the meaning is as stated.

non-linear in the sense that it did not proceed along a single well-defined path, iterative in that taxonomies were developed by successive approximations, and analytical where analysis was possible and judgment-based where conclusions could not be reached by straightforward analysis.

The dictionary definition of *analysis* refers to separating a whole into component parts and examining the elements and their relations (Merriam-Webster, 1986). Analyses often follow common steps of problem definition, decomposition into component parts, determining relations among elements, application of logical rules, and generation of conclusions. Developing the work taxonomies involved many if not all of these processes. Related analysis tasks included:

- Review existing taxonomies in, for example, job descriptions
- Combine and integrate existing taxonomies
- Assure taxonomies use consistent terminology and syntax
- Review nontaxonomy sources of information to synthesize taxonomy content
- Interview SMEs and others with job knowledge and experience to obtain information relating to taxonomy content
- Generate information content based on analyst knowledge and experience
- Level taxonomy elements to assure that taxonomy information content is assigned to the appropriate CWF, KA, or PI level
- Cluster taxonomy elements based on logical relationships, e.g., assigning related KAs to an existing CWF or creating a new CWF as needed
- Exclude information content that lies outside the analytical focus (federal civilians, journeyman level, technical)

The draft taxonomy defined the security profession (level 1 of the taxonomy) in terms of seven different disciplines (level 2): Physical Security, Information Security, Personnel Security, Security Investigations, Security Management, Communications Security, and Information Systems Security. Each of these disciplines, was defined at levels 3, 4, and 5 respectively in terms of its CWFs, KAs, and PIs.

Tippit et al. sent or personally delivered the draft taxonomy to personnel in several federal agencies and departments for informal review and comment and subsequently revised it based on feedback received.

CONDUCT SME WORKSHOPS

Overview

The workshops were envisioned as a way to advance the first two objectives of the project, namely, to vet the work taxonomies and to obtain input from SMEs that would enable development of skill standards.

The workshops were designed to unfold according to an agenda over 2-1/2 to 3 workdays in a conference room at the PERSEREC office in Monterey, CA, where small groups of SMEs would be free from distractions and able to dedicate their full attention to the work at hand. Each workshop was expected to involve 6-8 highly qualified SMEs, two facilitators, and an NSSB job analyst and to focus on a single security discipline.

Preworkshop Tasks

Because of the limited time available—most SMEs would come from the east coast and travel on Monday and Friday—it was necessary to plan the workshops to use time efficiently. SMEs would need to be familiar with the taxonomy when the workshop began. Further, it would be desirable for SMEs to review and critique the taxonomy beforehand to encourage independent judgment. Hence, a decision was made to request SMEs to perform three pre-workshop tasks: (1) review the taxonomy; (2) recommend any additions, deletions, or changes; and (3) identify any source documents that might be useful during the workshop (e.g., position descriptions, programs of instruction, job task analyses). SMEs needed to come to the workshop prepared and ready to present their ideas to their peers. A sample of the preworkshop tasking email that was sent to SMEs is shown as Exhibit B-1 in Appendix B.

Subject-Matter Experts

PERSEREC representatives contacted senior security personnel in DoD agencies and departments whose security staff had expertise in the security disciplines covered in the workshops, explained the purpose of workshops, and requested the agency or department to designate one or more SMEs on staff to participate. In addition, several retired senior security personnel were subcontracted to participate. Ultimately, 39 different SMEs participated in workshops. All had significant work experience, typically in a security career of 20+ years, often in more than a single discipline. One SME—formerly the Director of Defense Security Programs for OSD—participated in all seven workshops, provided continuity, and played a significant leadership role. Four other SMEs participated in at least two workshops. Exhibit B-2 in Appendix B lists the names and affiliations of SMEs for each security discipline.

Workshops

Schedule. Workshop disciplines, dates, and numbers of participating SMEs are shown in Table 5.

Table 5
Workshop Disciplines, Dates, and Numbers of Participating SMEs

Discipline	Dates	No. SMEs
Physical Security	8-10 July 2003	7
Information Security	9-11 September 2003	7
Personnel Security	9-11 December 2003	6
Security Investigations	8-10 June 2004	7
Security Management	24-26 August 2004	7
Communications Security	14-16 September 2004	7
Information Systems Security	26-29 October 2004	8

Conference Room Configuration. The workshop conference table was equipped with a laptop computer and coupled projector to enable a facilitator to annotate working documents and project them on a screen as SMEs reviewed them and reached consensus on needed additions, deletions, or changes. The agenda also provided for some small group work activities. Computers were available for SME use.

Agenda. In overview, the agenda for each workshop required the same set of work activities:

- SMEs individually presented recommended changes to the taxonomy to their peers followed by discussion and changes if consensus was reached
- SMEs reviewed source documents to determine if their information content should be reflected in the taxonomy
- SMEs conducted a final review of the taxonomy to align the language and syntax with NSSB standards
- SMEs participated in a working session with an NSSB job analyst to elicit K&S requirements and rate various dimensions of them

SMEs revised the taxonomy to describe security work as it is presently performed and did not attempt to describe how it might be performed in the future. The actual agenda also included some presentations and administrative, social, and procedural matters. A sample agenda is shown as Exhibit B-3 in Appendix B. The agenda, working materials, and procedures changed very little over the course of the seven workshops that were eventually conducted.

Ground Rules. Facilitators stated some ground rules before the first working session in each workshop. In summary, these were:

- Represent the profession, not the SME's home organization[7]

[7] Individuals from different organizations often express views reflecting the culture, philosophy, world view, and way of doing business of their organization. This may limit their willingness to accept the views of those from other organizations. Every one of the workshops involved SMEs from diverse backgrounds (see Exhibit B-2 in Appendix B) so

- Focus on technical tasks at journeyman level as they would be performed by federal civilians, contractors, and military personnel
- If an issue could not be resolved in discussion, the dissenting minority could issue its own report[8]
- SMEs' names would be associated with the skill standards produced by the workshop

SME Independence. One workshop objective was to have SMEs vet the work taxonomies. John Tippit, the taxonomies' principal author, presented an overview of the taxonomies and answered SME questions before SMEs reviewed them as a group. Tippit left before the SME review to assure that he did not influence their discussion and review.

It was important for SMEs to operate independently in other ways as well. PERSEREC facilitators provided the agenda, working materials, and procedures; kept track of time; and guided SMEs through a series of workshop activities, but deferred to SMEs in all technical matters. This philosophy included dealing with disagreements among workshop participants. Facilitators allowed SMEs to work out disagreements among themselves and did not inject themselves into discussion, offer solutions, or otherwise interfere with the decision-making dynamic. The closest they came on rare occasions was to suggest to the group that a point of disagreement seemed to exist and that the SMEs themselves needed to resolve it.

Work Materials. Facilitators provided SMEs with a set of working materials consisting of the draft taxonomy for the security discipline of interest, a handout explaining workshop terminology, and a list of concrete action verbs.

The taxonomy evolved in the workshop through several generations as SMEs revised it. Version 1 was based on the Tippit taxonomy but was reformatted from its original tabular format into a three-level outline. Exhibit B-4 in Appendix B illustrates the appearance of a typical taxonomy. Most literate adults are familiar with the concept of an outline and the hierarchical relationships among its different levels of information content. Tippit's tables were less intuitively obvious. Converting the tables to outlines also simplified editing with MS Word's outline view and editing commands. Exhibit B-4 has a title naming the discipline; a version number; a key illustrating taxonomy levels and content, with a short definition of CWF, KA, and PI; and the information content of the taxonomy.

there was concern that this might lead to conflicts. SMEs seemed able to overcome organizational biases and work effectively together. There is no way to know whether or not the facilitator's guidance had any effect on how SMEs conducted themselves in workshops. In any case, all of the SMEs were mature professionals who probably understood the need to look beyond their home organization.

[8] There were no unresolved discussions, and no workshop minority ever issued a minority report.

The *Workshop Terminology* handout is shown as Exhibit B-5 in Appendix B. The handout defines CWF, KA, and PI terminology; gives concrete examples; and illustrates the syntax of valid CWF, KA, and PI statements. It provided SMEs with examples to use when revising or composing CWF, KA, and PI statements. This handout was developed after the first workshop and used in all subsequent workshops.[9]

The *List of Concrete Action Verbs* is shown as Exhibit B-6 in Appendix B. The list was based on an NSSB list and provided SMEs with examples of the types of verbs appropriate for use in constructing CWF, KA, and PI statements.

Facilitators used a set of workshop procedures analogous to a teacher's lesson plan (Exhibit B-7 in Appendix B) and also had a table containing SME names, affiliations, and contact information.

Revising the Taxonomy. The majority of workshop time was spent in discussion and reaching consensus on revisions needed to the taxonomy. SMEs first reviewed the taxonomy as a group to vet its CWFs, KAs, and PIs. Next, they formed small groups and reviewed job-related documentation and incorporated relevant information content in the taxonomy. The last step was to go through the taxonomy from beginning to end and align its language and syntax based on the guidance in Exhibits B-6 and B-7.

Obtaining SME Ratings. After revising the taxonomy, the focus shifted to obtaining SME ratings. In all cases, ratings were obtained in a group setting, facilitated by the NSSB job analyst, and made verbally and by consensus rather than individually using paper instruments.[10]

SMEs first estimated the *knowledge* levels required to perform each KA for entry-level, journeyman, and senior security professionals in each discipline using a four-level scale. The scale used is described in the next section, *Skill Standards Overview*, and in Appendix C, and to avoid redundancy will not be repeated here. This is also true for the other rating scales mentioned below. Readers who want to examine the scales should refer to *Skill Standards Overview* or Appendix C.

[9] The first workshop, on physical security, did not use NSSB terminology but the same terminology as the Tippit et al. report (i.e., discipline, major functions, function elements, major tasks), which had to be translated for users into terms more commonly used (i.e., occupation, duties, tasks, subtasks), and later translated by the NSSB analyst into NSSB terminology (discipline, CWF, KA, PI) when skill standards were developed. In effect, three different sets of terminology were in use concurrently. Doing this was unduly cumbersome and a decision was made after the first workshop to use the NSSB terminology exclusively. This experience was an object lesson in how job analysis can become tangled up in words.

[10] The small number of SMEs involved would have made it difficult to obtain valid and reliable ratings by combining ratings made by individual SMEs acting independently. The results of the rating by consensus method used should be considered an approximation.

SMEs next estimated the *performance* levels required on each KA using a four-level scale.

SMEs then reviewed the set of 23 NSSB A&E K&S[11] and judged whether they were *important* or *not applicable* to performance at different seniority levels for each security discipline. SMEs also judged whether or not each A&E K&S was relevant to effective performance on each discipline's CWFs.

The NSSB job analyst derived a set of OTKS for each discipline based on the taxonomy and working sessions with SMEs. This was done during the workshop and after hours. The OTKS apply to workers at all levels of seniority, but OTKS *complexity* increases with seniority. OTKS may also vary in how they affect performance on different CWFs. SMEs estimated the complexity levels required for each OTKS for entry-level, journeyman, and senior professionals in each security discipline using a five-point scale. SMEs also judged whether or not each OTKS is relevant to effective performance on the CWFs for each security discipline.

Refining Workshop Procedures. The first workshop, on Physical Security, served as a pilot to test workshop procedures and work materials. The project manager, facilitators, and the NSSB job analyst participated in an extended discussion with SMEs at the end of the workshop to review and critique the workshop and determine lessons learned and how to improve future workshops. Following that workshop, workshop terminology, procedures, and work materials were modified. As already noted, terminology was simplified and made uniform (see footnote 9), the taxonomy was reformatted from tabular to outline format to facilitate editing, the ground rules were formalized and documented for future presentation to SMEs, and some handouts which were found to be superfluous were eliminated. Overall, these changes were relatively minor.

DERIVE SKILL STANDARDS

Postworkshop Review of Draft Skill Standards

After each workshop, the NSSB job analyst prepared draft sets of skill standards for further review. What happened next differed for the first two and last five workshops.

After the first two workshops (covering Physical and Information Security), the draft standards were reviewed by a Functional Panels of "seniors" organized and facilitated by the JSTC. Panel members were persons with extensive experience and recognized national standing in the particular security discipline who represented

[11] Academic K&S are associated with the academic disciplines of reading, writing, mathematics, and science. Employability K&S are general workplace K&S such as such as teamwork, decision making, and problem solving. The combination is referred to as "A&E K&S". The NSSB developed a set if A&E K&S and we used it directly. A&E K&S are described in greater detail in the section titled Skill Standards Overview.

key federal agencies. The standards were then posted on the JSTC web site for further review by the security community, but the response was sparse and the outcome unproductive. JSTC changed management in early 2004 and discontinued supporting the use of functional panels.

The remaining five workshops (covering Personnel, Communications, and Information Systems Security; Security Investigations; and Security Management) were conducted without functional panels or web page posting and relied entirely upon work done by the participating SMEs in the workshops, post-workshop review via email, and communication via telephone or teleconference.

Generating NSSB-Formatted Skill Standards

After postworkshop review of the draft standards by functional panel or SMEs, the NSSB job analyst integrated the information generated into a complete set of skill standards for each security discipline using NSSB information presentation formats. At this stage, the skill standards were complete in terms of information content (although none had been subjected to a field validation survey). The NSSB formatted standards ranged in length by discipline from 37 to 60 pages with a total length of 321 pages.

Skill Standards Information Design

The NSSB skill standards information presentation formats had several shortcomings that would make them difficult for end-users to understand, navigate, interpret, or apply. The most serious were low information density; unnecessary repetition of definitions and information content; and the use of color, numeric, and letter codes to the exclusion of graphics.

To overcome these shortcomings, the information presentation formats were redesigned to increase their information density, eliminate unnecessary repetitions, and use graphics rather than color, numeric, or letter codes. When reformatted, the skill standards comprised about 60 percent of their former volume and did not require color code key cross-referencing to interpret. Reviewers who had worked with both the NSSB and redesigned skill standards commented positively on the changes made.

SKILL STANDARDS OVERVIEW

OVERVIEW AND SUGGESTED READING STRATEGY

This section provides an introduction and overview of the skill standards. It describes the structure, content, and format of the standards with brief excerpts of the information content to illustrate. The complete skill standards are contained separately in Appendices D through J of this report:

- Appendix D. Communication Security
- Appendix E. Information Security
- Appendix F. Information Systems Security
- Appendix G. Personnel Security
- Appendix H. Physical Security
- Appendix I. Security Investigations
- Appendix J. Security Management

The appendices are designed for end-users of the standards such as trainers, training evaluators, training designers, job performance evaluators, job designers, and developers of certification programs. This section is duplicated in Appendix C so that end-users can remove it and appendices D-J and use the combination in stand-alone fashion. End-users of the standards may safely skip this section and go directly to Appendix C and other appendices for the security disciplines of interest.

STRUCTURE OF THE STANDARDS

The skill standards fall into two broad categories:

- Work-oriented component—what the worker does to perform the job successfully
- Worker-oriented component—what knowledge and skills (K&S) the worker requires to perform the job successfully

SUBJECT-MATTER EXPERT NOTES

SMEs who helped develop the skill standards sometimes attached explanatory notes to them. The notes, if provided, vary among standards, but addressed issues that the SMEs thought were important but not covered within the standards themselves.

GENERAL PERFORMANCE EXPECTATIONS AND SENIORITY LEVEL

General performance expectations by worker seniority level are summarized in Table 6.

Table 6
General Performance Expectations by Worker Seniority Level

Seniority Level		
Entry	**Journeyman**	**Senior**
• Work as a team member • Perform task-level work (associated with key activities) competently • Require major supervision	• Work independently • Perform function- or project-level work at full performance level • Mentor entry-level individuals	• Direct technical work of others • Perform work at the system-level • Serve the role as technical subject-matter expert

WORK-ORIENTED COMPONENT

Definitions

The work-oriented component is described in each set of standards in the form of a three-level taxonomy or outline structured as shown below.

Top Level - Critical Work Functions (CWF1, CWF2, etc.)
Second Level - Key Activities (KA1, KA2, etc.)
Third Level - Performance Indicators (PI)

Table 7 defines taxonomy terms, gives examples, and illustrates CWF, KA, and PI statement syntax.

Table 7
Taxonomy Terminology, Examples, and Syntax

Term	**Definition**	**Example**	**Syntax**
Critical Work Function (CWF)	Major responsibilities of work	Define Personnel Security Standards	Action verb + Object
Key Activity (KA)	Major duties or tasks involved in carrying out a CWF	Delineate Employment and Associational Requirements	Action verb + Object
Performance Indicator (PI)	Provides information to judge whether a KA is performed competently	“Employment” security standards are identified, defined, and monitored	Object + Action verb (passive voice)

CWF and KA statements consist of an action verb followed by an object and are written in the *active* voice. PI statements consist of an object followed by an action verb and are written in the *passive* voice. PI statements are concrete actions. KA performance can be judged based on whether or not and how well the underlying PIs are performed.

Example of a Taxonomy

Figure 1 is an excerpt from the Personnel Security taxonomy. Note that CWF statements are preceded by "CWF" and numbered. KA statements are preceded by "KA" and numbered. PI statements are listed below KA statements without the "PI" label and are unnumbered.

CWF1: Define Personnel Security Standards

- KA1: Delineate Employment and Associational Requirements
    - "Employment" security standards are identified, defined, and monitored
    - Third-party contractor security standards are identified, defined, and monitored
    - Legal and regulatory constraints, if any, are identified, reviewed, and monitored
    - Program plans and/or processing requirements are developed
- KA2: Apply National Security Clearance and/or Specialized Access Requirements
    - Requirements and/or "specialized access" provisions are identified, defined, and monitored
    - Program objectives and processes are identified and developed
    - Legal and regulatory constraints, if any, are identified, reviewed, and monitored
    - Program plans and/or processing requirements are developed
- KA3: Apply Reliability and/or Suitability Concerns
    - High risk task elements requiring greater reliability and/or suitability concerns are identified, defined, and monitored
    - Participation in the determination and evaluation of job sensitivity designations are met
    - Program objectives and processes are identified, defined, and monitored
    - Legal and regulatory constraints, if any, are identified, reviewed, and monitored
    - Program plans and/or processing requirements are developed

Figure 1 Excerpt of the Personnel Security Taxonomy

Key Activity Knowledge and Performance Level Expectations by Seniority

SMEs estimated the *knowledge* levels required to perform each KA for entry-level, journeyman, and senior security professionals in each discipline using the A-D scale shown in Table 8.

Table 8
KA Knowledge Level Scale Definitions

Scale	Description
D-advanced theory	Able to predict, isolate, and resolve problems about the key activity
C-operating principles	Able to identify why and when the key activity must be done and why each step is needed
B-procedures	Able to determine step-by-step procedures for doing the key activity
A-nomenclature	Able to name parts, tools, and simple facts about the key activity

Note that each knowledge level includes all levels below it. For example, a worker with *C-operating principles* proficiency must also possess proficiency at *B-procedures* and *A-nomenclature.*

SMEs also estimated the *performance* levels required on each KA using the 1-4 scale shown in Table 9.

Table 9
KA Performance Level Scale Definitions

Scale	Description
4-highly proficient	• Able to complete the KA quickly and accurately • Can tell or show others how to do the KA
3-competent	• Able to do all parts of the KA • Needs only a spot check of completed work
2- partially proficient	• Able to perform most parts of KA • Needs only help on hardest parts
1- extremely limited	• Able to perform simple parts of the KA • Needs to be told or shown how to do most of the KA

Note that each performance level is discrete. Typically, a worker at the *4-highly proficient* level has progressed above *3-competent* and lower levels and performance is no longer accurately described with lower scale levels.

Table 10 is an excerpt of a table summarizing SME estimates of knowledge and performance levels required on KAs in relation to seniority level for Personnel Security. The left column lists KAs by number, the next three columns to the right show Knowledge level by Seniority, and the three columns on the far right show Performance level by Seniority. Consider the entries to be the minimums required for a worker at each seniority level. Cell entries in the table may be viewed as both text and bar graphs. It is apparent that workers are expected to increase both knowledge and performance level as they gain seniority.

Table 10
Excerpt of a Table Summarizing Knowledge and Performance Levels Required on Kas in Relation to Seniority Level for Personnel Security

Key Activity	Knowledge Level by Seniority			Performance Level by Seniority		
	Entry	Journeyman	Senior	Entry	Journeyman	Senior
1. Delineate Employment and Associational Requirements	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
2. Apply National Security Clearance and/or Specialized Access Requirements	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
3. Apply Reliability and/or Suitability Concerns	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
4. Apply Qualification and Reliability Standards	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high

WORKER-ORIENTED COMPONENT

Definitions

The Worker-Oriented Component consists of three types of K&S: Academic, Employability, and Occupational and Technical. These terms are defined in Table 11.

Table 11
Three Types of K&S in Worker-Oriented Component of Skill Standards

Type of K&S	Definition
Academic	K&S associated with the academic disciplines of reading, writing, mathematics and science
Employability	K&S such as teamwork, decision making, and problem solving that apply across a broad ranges of occupations
Occupational and Technical	K&S that apply to the specific type of work

Academic and Employability K&S are combined and called “A&E K&S.” Occupational and Technical K&S are called “OTKS.”

Academic and Employability K&S

There are 23 A&E K&S. Their importance may vary for performance at entry, journeyman, and senior levels. They may also vary in how they affect performance on different CWFs. SMEs reviewed the A&E K&S and judged whether they were *important* or *not applicable* to performance at different seniority levels for each security discipline. SMEs also judged whether or not each A&E K&S was relevant to effective performance on each discipline’s CWFs.

Table 12 shows importance by seniority and relevant CWFs for the first three A&E K&S for Personnel Security. The left column lists and defines each A&E K&S. The next three columns to the right show Importance by Seniority as either important (●) or not applicable (n/a). The eight columns on the far right indicate that the A&E K&S is relevant to the CWF by the presence of a CWF number or not relevant with a blank. (Personnel Security has a total of eight CWFs, but the number varies among disciplines.)

Table 12
Importance by Seniority and Relevant CWFs for Three A&E K&S for Personnel Security

Academic & Employability Knowledge & Skills	Importance by Seniority			Relevant CWFs							
	Entry	Journeyman	Senior	1	2	3	4	5	6	7	8
1. Ability to Learn—Recognize and use learning techniques and recall available information to apply and adapt new knowledge and skills in both familiar and changing situations. Use multiple approaches when learning new things. Assess how one is doing when learning or doing something. Keep up to date technically and know one's own job and related jobs.	●	●	●	1	2	3	4	5	6	7	8
2. Adaptability—Change one's own behavior or work methods to adjust to other people or to changing situations or work demands; be receptive to new information, ideas or strategies to achieve goals.	●	●	●	1	2	3	4	5	6	7	8
3. Analyzing and Solving Problems—Anticipate or identify problems and their causes; develop and analyze potential solutions or improvements using rational and logical processes or innovations and creative approaches when needed.	●	●	●	1	2	3	4	5	6	7	8

Occupational and Technical K&S

Occupational and Technical K&S apply to the specific type of work. Think of them as what the worker must know and be able to do to perform competently. The OTKS apply to workers at all levels of seniority, but OTKS *complexity* increases with seniority. OTKS may also vary in how they affect performance on different CWFs.

SMEs estimated the complexity levels required for each OTKS for entry-level, journeyman, and senior professionals in each security discipline using the 1-5 scale shown in Table 13.

SMEs also judged whether or not each OTKS is relevant to effective performance on the CWFs for each security discipline.

Table 13
OTKS Complexity Level Scale Definitions

Scale	Description
5-expert/master K&S required	• Requires ability to independently apply K&S in the most complex, difficult, novel, stressful, or unexpected situations, or situations with high consequences for error • Requires the ability to supervise or lead others in the application of this K&S • Roughly equivalent to the K&S level typically attained through a combination of extensive specialized training or education and an advanced or graduate degree, or at least five years of direct application or use of this knowledge or skill.
4-advanced K&S required	• Requires ability to independently apply K&S in moderately complex, difficult, or stressful situations or situations with moderately high consequences for error • Requires the ability to assist others in the application of this K&S • Roughly equivalent to the K&S level typically attained through extensive specialized training or education or an undergraduate degree or major, or at least two years of direct application or use of this knowledge or skill
3-working or operational K&S required	• Requires ability to independently apply K&S across a range of common applications to meet typical work requirements and having moderate consequences for error • Roughly equivalent to the K&S level typically attained through multiple training courses or a two-year or technical school degree, or 6–24 months of direct application or use of this knowledge or skill
2-basic K&S required	• Application of K&S is limited to relatively routine situations with frequent assistance of others and/or close supervision, and somewhat low consequences of error • Roughly equivalent to the K&S level typically attained through one or two training or academic courses or 1 - 6 months of direct application or use of this knowledge or skill
1-limited K&S required	• General familiarity or awareness of basic concepts or fundamentals, but little or no practical experience • Application of K&S is limited to highly routine, simple, and closely supervised situations with very low consequences of error • Roughly equivalent to the K&S level typically attained through indirect work experience (e.g., observation of others) or less than one month of direct application of this knowledge or skill

Table 14 shows Complexity Level by Seniority and Relevant CWFs for the first three Personnel Security OTKS. The left column lists each OTKS, the next three columns to the right show Complexity Level by Seniority, and the eight columns on the far right indicate that the OTKS is relevant to the CWF by the presence of a CWF number or not relevant with a blank. Complexity Level by Seniority cell entries may be viewed as both text and bar graphs. It is apparent that workers are expected to deal with increasing complexity as they gain seniority. Complexity entries that indicate two levels represent a range. Consider the entries to be the minimums required for a worker at each seniority level.

Table 14
Complexity by Seniority and Relevant CWFs for Three Personnel Security OTKS

Occupational & Technical Knowledge & Skills	Complexity Level by Seniority			Relevant to CWFs							
	Entry	Journeyman	Senior								
1. Policies, regulations, guidelines and ethical standards that govern the conduct of Personnel Security Investigations (including, but not limited to): • Investigative standards • Section 1001 and 1905, Title XVIII US Code and other applicable laws • DCID 6/4 • EO 12968 • EO 10450 • Privacy Act 1974 & Freedom of Information Act • Ethical standards (prohibitions and forbidden topics) • Other policies and directives	2-basic 1-limited	3-working	5-expert 4-advanced	1	2	3	4	5	6	7	8
2. Adjudicative guidelines • Allegiance to the United States • Foreign influence • Foreign preference • Sexual Behavior • Personal Conduct • Financial considerations • Alcohol consumption • Drug involvement • Emotional, mental, personality disorders • Criminal conduct • Security violations • Outside activities • Misuse of information technology systems	1-limited	3-working	5-expert	1		3	4	5	6	7	8
3. Investigation concepts, principles, and practices (including, but not limited to): • Types of investigations • Scope of investigations • Coverage requirements for each type of investigation (e.g., Single Scope Background Investigations (SSBI) and SSBI-Periodic Reinvestigations)	1-limited	4-advanced 3-working	5-expert 4-advanced	1		3	4	5	6	7	8

APPLYING THE SKILL STANDARDS

INTRODUCTION

Overview

This section is for end-users of skill standards such as trainers, training evaluators, training designers, job performance evaluators, job designers, and developers of certification programs. It provides guidance to help them use the skill standards in five specific applications: training definition, training assessment, job performance evaluation, job definition, and certification. This section describes the five applications, discusses several considerations that apply to all of them, and then describes and illustrates each application in more detail.

It is important to understand skill standards terminology, abbreviations, and what the skill standards are before reading this section. Carefully review the previous section, *Skill Standards Overview* or Appendix C before starting the present section.

The Five Applications

Training Definition is the process of deciding what to cover in training. *Training Assessment* is the process of assessing training that already exists. *Performance Evaluation* is the process of evaluating how well a worker performs the job. *Job Definition* is the process of defining a particular type of job. *Certification* is the process of determining whether or not a worker is able to meet criteria and standards required for certification.

Each of the five applications asks slightly different questions. *Training Definition* asks what training should cover, *Training Assessment* asks whether existing training covers what is needed, *Performance Evaluation* asks whether a worker can perform competent work, *Job Definition* asks what workers must do on the job, and *Certification* asks whether a worker is able to meet criteria and standards required for certification. While the questions differ, in each case, the skill standards provide important information that can help answer each question. In addition, the Certification application contains elements of both the Training Assessment and Performance Evaluation applications.

Cautionary Notes

Performing these applications requires relevant technical and professional background and experience. Most require more than subject-matter expertise. Some of the applications—such as performance evaluation and certification—have significant legal implications. For example, employees may legally contest employment actions (e.g., promotion, job assignments) made by agencies based on performance evaluations whose validity is questionable.

It is safe to regard the skill standards as a reasonable description of the work performed in each security discipline and the K&S that workers need to perform it competently. Keep their limitations in mind. First, they describe disciplines, not jobs. Second, they are unvalidated through field surveys of job incumbents; conducting such surveys may be important in high-stakes applications such as certification and performance evaluation.[12] Third, they describe the disciplines based on a snapshot in time representing roughly the year 2004.[13]

The Five Skill Standards

Skill standards describe (1) the work performed on a job and (2) the K&S workers need to perform it competently. Skill standards use scales and specify required levels of knowledge and performance at different seniority levels. The five standards, their scales, and typical proficiency at entry, journeyman, and senior levels are shown by text and shading in Table 15. The "typical" proficiencies shown are approximations based on the prevailing patterns in many different skill standards. Actual proficiencies are based on SME ratings and often vary from "typical" proficiencies. Consider the cell entries for standards 2, 3, and 5 to be the minimums required for a worker at each seniority level and may be viewed as both text and bar graphs. It is apparent that workers are expected to increase in knowledge and performance level and in the complexity they handle as they gain seniority.

Standard 1, *Taxonomy*, is an inventory of the CWFs, KAs, and PIs for a particular security discipline. All workers are expected to perform a subset of these that depends upon their specific job assignment. Worker independence and level of responsibility usually vary with seniority, as shown in the table. KAs are major duties or tasks and how people usually describe jobs. CWFs are labels used to group KAs with commonalities. KAs in turn consist of PIs, which may also be thought of as KA subtasks. KA performance can be assessed in part based on whether or not and how well the underlying PIs are performed.

Standard 2, *KA Knowledge Level*, has a four-level scale, and knowledge level usually increases with seniority as shown in Table 8.

Standard 3, *KA Performance Level*, has a four-level scale, and performance level usually increases with seniority as shown in Table 9.

Standard 4, *A&E K&S Importance*, has a two-level importance scale. All A&E K&S are usually important at all seniority levels with the possible exceptions of science

[12] The conduct of such surveys is beyond the scope of this report but is discussed in more detail in *Discussion and Conclusion.*

[13] The standards were based on a descriptive analysis (describing how something is) rather than a strategic analysis (describing how something will be in the future) and will need to be updated periodically.

and, for entry-level workers, leadership. The importance scale is quite complex and is not described in this report.[14]

Table 15
Skill Standards, Scales, and Typical Proficiency by Seniority

Skill Standard	Typical Proficiency by Seniority		
	Entry	Journeyman	Senior
1. Taxonomy (CWFs, KAs, & PIs)	• Work as a team member • Perform task-level work (associated with key activities) competently • Require major supervision	• Work independently • Perform function- or project-level work at full performance level • Mentor entry-level individuals	• Direct technical work of others • Perform work at the system-level • Serve the role as technical subject-matter expert
2. KA Knowledge Level	D-advanced theory C-operating principles B-procedures A-nomenclature	D-advanced theory C-operating principles B-procedures A-nomenclature	D-advanced theory C-operating principles B-procedures A-nomenclature
3. KA Performance Level	4-highly proficient 3-competent 2- partially proficient 1- extremely limited	4-highly proficient 3-competent 2- partially proficient 1- extremely limited	4-highly proficient 3-competent 2- partially proficient 1- extremely limited
4. A&E K&S Importance	all important except 8. leadership and 15. science	all important except 15. science	all important except 15. science
5. OTKS Complexity	5-expert 4-advanced 3-working 2-basic 1-limited	5-expert 4-advanced 3-working 2-basic 1-limited	5-expert 4-advanced 3-working 2-basic 1-limited

CWF – Critical Work Function
KA – Key Activity
PI – Performance Indicator
A&E K&S – Academic and Employability Knowledge and Skill
OTKS – Occupational and Technical Knowledge and Skill

Standard 5, *OTKS Complexity*, has a five-level scale, and complexity level usually increases as shown in Table 13. The complexity scale is defined in more detail in Table 13.

Narrowing the Focus

The skill standards for any security discipline in Appendices D through J are quite lengthy and ideally tell everything about all the work performed and all the K&S needed to perform it for all workers at all seniority levels. However, in any specific application, the end-user will probably want to focus more narrowly on some part of the work (e.g., a subset of all the CWFs, KAs, and PIs) and related K&S and on workers at one rather than all seniority levels. For example, in performing an application such as training definition, one might want to focus on a relatively small number of KAs for entry-level workers. Deciding what to include and exclude

[14] The importance scale is described fully in *Skill Scales Companion Guide* (National Skill Standards Board, 2000b) (http://www.tssb.org/wwwpages/SkillScalesCompanionGuide.pdf).

is an important step and should be done with care. This may be done in various ways. Some possibilities are:

- A group of SMEs decides based on consensus
- Analysts decide in consultation with SMEs
- Analysts survey the security community to determine its needs and preferences and decide based on survey findings
- Policymakers decide
- Supervisors decide based on the training needs or performance requirements of their subordinates

The end-user must use judgment—alone or with others in a position to know—to narrow the focus. The more rigorously this is done, the better. Nonetheless, the process is subjective and the outcome will only be as good as the judgment of the people who participate in the process.

There are no strict rules about which skill standards to use in performing an application. Moreover, applications may vary in scale and focus, and different end-users may make different choices. Nonetheless, readers may find it interesting to know what choices the authors made in describing and illustrating the applications later in this section. The skill standards used in the five applications are shown in Table 16.

Skill standards 1, 2, and 3—which basically describe what workers do on the job and how proficiently—were used in all applications. Skill standard 5 was used in all applications except Performance Evaluation, from which it was excluded because it is not directly observable as a performance. Skill Standard 4 was excluded from three applications because it deals with academic and general workplace rather than technical proficiencies. It was used in the Job Definition and Certification applications, but even there it appeared to be optional rather than required.

Table 16
Use of Skill Standards in Five Common Applications

Skill Standard	**Application**				
	Training Definition	**Training Assessment**	**Performance Evaluation**	**Job Definition**	**Certification**
1. Taxonomy (CWF, KAs, & PIs)	●	●	●	●	●
2. KA Knowledge Level	●	●	●	●	●
3. KA Performance Level	●	●	●	●	●
4. A&E K&S Importance	n/a	n/a	n/a	○	○
5. OTKS Complexity	●	●	○	●	●

● – applicable ○ – may be applicable n/a – not applicable

Application Tools

The skill standards are the starting point in performing an application. The information contained in the standards can be used directly, though it will usually be more practical to develop application tools based on the standards. Examples of application tools are paper- or computer-based forms such as checklists, rating forms, task or KA lists, written tests, performance test protocols, lists of training objectives or requirements, job descriptions, and job classification standards. Model application tools are presented as examples in the discussion of each of the five applications, below.

Application Terminology

The skill standards in this report were drafted using NSSB terminology, which is somewhat at variance with common usage. End-users who apply the standards may find it helpful to translate the NSSB terminology to facilitate clarity. Table 3, presented earlier in the *Job Analysis* section, compares NSSB and traditional terminology. For example, KAs are more commonly referred to as “tasks”, PIs may be interpreted as tasks in their own right but are more commonly called “task elements” or “subtasks”. Readers should feel free to modify the terminology if it makes it easier to perform their application. In drafting this section, the authors made slight modifications in some terminology and also found it helpful in some applications to convert PIs from passive to active voice.

APPLICATION 1. TRAINING DEFINITION

Training Definition is the process of deciding what to cover in training. Its product is a set of *training objectives*, which can be used to design and develop training. Professional training developers generally define training quite systematically, often by using the Instructional Systems Development (ISD) or other formal training development approach. Workplace supervisors are typically expected to define training for their subordinates, although they may lack the resources and know-how to apply a formal training development approach. Regardless of setting, however, skill standards can help one define training. While it is impractical for every trainer to apply the ISD approach, it is enlightening to see how ISD fits skill standards into the training definition picture. Butler (1972) describes ISD as a multi-step process starting with a feasibility study and then a job task analysis that defines the “activities, knowledge, skills, environment, tools, aids, equipment, and standards.” The next step is to develop training objectives, which define what trainees are expected to be able to do after completing training in terms of specific behaviors, performance conditions, and performance standards (Mager, 1962, 1997).[15] The training objectives are then used to develop the various components of

[15] Training objectives are also commonly called “learning objectives” or “skill and knowledge requirements”. Some authors distinguish between *enabling* and *terminal* objectives. Enabling objectives are less rigorous than terminal objectives and may, for example, describe expected trainee performance during training whereas terminal

training, such as tests, learning strategies, instructional sequencing, and lessons. Note that the skill standards effectively accomplish everything leading up to the training objectives and the next step in defining training is to develop training objectives.

Narrowing the Focus

Assume for the sake of discussion that a group of trainers wants to develop introductory training for entry-level workers in the personnel security discipline and to focus on a single CWF and its underlying KAs. The complete set of skill standards for personnel security is contained in Appendix G. These standards cover all work performed and K&S needed for workers at all seniority levels. Let us narrow the focus by concentrating only on CWF1 (Define Personnel Security Standards) and entry-level workers. If one needs to focus training for a particular group of workers, their current performance levels and training needs should also be taken into account. The standards of greatest interest are 1 (Taxonomy), 2 and 3 (KA Knowledge and Performance Levels, and 5 (OTKS Complexity). Standard 4 (A&E K&S) is excluded because it reflects academic and general workplace proficiencies rather than technical ones and would probably not be covered in introductory training.[16]

The next step is not required but probably a good idea. It is to reformat the standards in Appendix G by extracting only the information necessary in the application. Doing this considerably reduces the amount of paper and extraneous information and makes it easier to find what is needed to develop training objectives. Reformatting reduces everything to two tables. Table 17 combines Skill Standards G-1 and G-2 and shows the KAs and PIs for CWF1 and the required knowledge and performance levels for entry-level personnel only. Skill Standard G-3 (A&E K&S) is not used. Table 18 is based on Skill Standard G-4, but includes only OTKS that apply to CWF1 and complexity scales for entry-level personnel. It is recommended that readers compare Tables 17 and 18 with the skill standards in Appendix G to see how they were compiled.[17]

objectives describe performance at the conclusion of training. Skill standards can be used to develop either type of objective but the current discussion deals with terminal objectives.

[16] Readers must decide if the standard is relevant in this and other applications. To the authors it seemed unlikely that end-users would want to investigate worker academic K&S such as mathematics or reading, or employability K&S such as interpersonal skills or working in teams.

[17] In interpreting Tables 17 and 18, recall that each KA knowledge level includes all levels below it, each KA performance level is discrete, and that multiple OTKS complexity entries represent a range. These scales are explained in greater detail in *Skill Standards Overview* and *Appendix C.*

Table 17
Key Activities, Performance Indicators, and Required Knowledge and Performance Levels for Entry-Level Security Practitioners Performing Personnel Security CWF1

Note: Entry-level security practitioners are expected to (1) work as team members, (2) perform task-level work (associated with key activities) competently, and (3) require major supervision

Critical Work Function	Key Activities	Performance Indicators	Required Knowledge Levels	Required Performance Levels
CWF1: Define Personnel Security Standards	1. Delineate Employment and Associational Requirements	• "Employment" security standards are identified, defined, and monitored • Third-party contractor security standards are identified, defined, and monitored • Legal and regulatory constraints, if any, are identified, reviewed, and monitored • Program plans and/or processing requirements are developed	B-procedures A-nomenclature	2-partial
	2. Apply National Security Clearance and/or Specialized Access Requirements	• Requirements and/or "specialized access" provisions are identified, defined, and monitored • Program objectives and processes are identified and developed • Legal and regulatory constraints, if any, are identified, reviewed, and monitored • Program plans and/or processing requirements are developed	B-procedures A-nomenclature	2-partial
	3. Apply Reliability and/or Suitability Concerns	• High risk task elements requiring greater reliability and/or suitability concerns are identified, defined, and monitored • Participation in the determination and evaluation of job sensitivity designations are met • Program objectives and processes are identified, defined, and monitored • Legal and regulatory constraints, if any, are identified, reviewed, and monitored • Program plans and/or processing requirements are developed	B-procedures A-nomenclature	2-partial

Table 18
Occupational and Technical Knowledge and Skill Complexity Levels Required for Entry-Level Security Practitioners Performing Personnel security CWF1

Occupational and Technical K&S	Complexity Level
1. Policies, regulations, guidelines and ethical standards that govern the conduct of Personnel Security Investigations (including, but not limited to): • Investigative standards • Section 1001 and 1905, Title XVIII US Code and other applicable laws • DCID 6/4 • EO 12968 • EO 10450 • Privacy Act 1974 & Freedom of Information Act • Ethical standards (prohibitions and forbidden topics) • Other policies and directives	2-basic 1-limited
2. Adjudicative guidelines • Allegiance to the United States • Foreign influence • Foreign preference • Sexual Behavior • Personal Conduct • Financial considerations • Alcohol consumption • Drug involvement • Emotional, mental, personality disorders • Criminal conduct • Security violations • Outside activities • Misuse of information technology systems	1-limited
3. Investigation concepts, principles, and practices (including, but not limited to): • Types of investigations • Scope of investigations • Coverage requirements for each type of investigation (e.g., Single Scope Background Investigations (SSBI) and SSBI-Periodic Reinvestigations)	1-limited
4. Case and time management strategies	2-basic 1-limited
5. Information elicitation techniques (including, but not limited to): • Policies regarding telephonic interviews • Handling requests for presence of representation during interviews	2-basic 1-limited
12. Concepts, principles, and practices associated with the application of adjudicative criteria, disqualifying factors, and mitigating factors	1-limited
13. Agency-specific terminology, structure, instructions, correspondence procedures, or regulations	1-limited
14. Levels of clearance and access	3-working 2-basic 1-limited
15. Interim access criteria and justifications	1-limited
16. Terminologies (including, but not limited to): • Medical/mental health terminology • Financial terminology • Legal terminology • Alcohol/Drug terminology • Criminal behavior terminology • Immigration and naturalization terminology	2-basic 1-limited

Occupational and Technical K&S	Complexity Level
17. Special Program case procedures (including, but not limited to): • Special Access programs	1-limited
18. Physical security requirements associated with personnel security	1-limited
19. Computer and information systems usage guidelines (including, but not limited to): • IT-based applications related to personnel security (proper use, rules and guidelines)	1-limited
23. Concepts and principles of clearance, access, reliability, suitability, and trustworthiness	1-limited
24. Ethical issues associated with personnel security	2-basic 1-limited
26. Third party release provisions	1-limited
27. Risk management concepts, principles, and practices	1-limited
28. Record management requirements as related to personnel security	1-limited
29. Information Assurance requirements as related to personnel security	1-limited
30. Information System Security requirements as related to personnel security	1-limited
31. Operations Security Program requirements as related to personnel security	1-limited
32. Personnel security-related funding, manpower requirements, and budgeting programs	1-limited
34. Personnel security regulations and processes including protected information status, determination, assessment procedures, security, marking, control, accountability, and safeguarding of records	1-limited
35. Preparation, coordination, and execution of MOU, MOA, Interservice Support Agreements, and Service Level Agreements	1-limited
36. Program evaluation concepts, methods, and techniques	1-limited
37. National disclosure policies	2-basic 1-limited
39. Development, preparation, and execution of personnel security plans	1-limited
40. Development, preparation, and execution of personnel security policies and procedures	1-limited
43. Methods for analyzing, organizing, compiling, and reporting personnel security data	1-limited

Developing Training Objectives

Training objectives define what trainees are expected to be able to do after completing training in terms of specific tasks, conditions, and performance standards. The skill standard equivalent of a *task* is a KA. In addition, PIs may be interpreted as tasks in their own right but are more accurately described as subtasks. The NSSB convention is to write PIs in the passive voice, whereas Mager and others instruct training developers to write training objective tasks or subtasks in the active voice, starting with an action verb that is followed by a statement that describes an observable behavior. For example, the first PI for KA1 in the Personnel Security discipline is *"Employment" security standards are identified, defined, and* *monitored.* This PI can be restated in the active voice as *Identify, define, and monitor "Employment" security standards.*

The *condition* in a training objective is the condition under which the performance will occur, including any tools or job aids, limitations, and so forth. Most of the skill standards do not provide information on conditions. Some exceptions are those that identify specific documents or tools needed to perform.

The *standard* in a training objective is the performance level required after training. The skill standards contain standards of performance for all of the KAs, A&E K&S, and OTKS that can, in turn, be used in training objectives.

One way to draft training objectives is to write separate objectives for each task, each with it own task statement, conditions, and standards. This works well with a small number of discrete tasks but is cumbersome with a large number of related tasks and subtasks. A more economical way to convey the same information is to present the tasks and subtasks in tabular form, accompanied by general statements about the related conditions and standards. This is the form used in the model set of training objectives presented below. The training objectives are based on the skill standards information in Tables 17 and 18. Note that this is not a program of instruction but can be used for developing training. The boxed information provides a general description of the objectives in terms of a Title, Scope, and Prerequisites and then presents the objectives in terms of tasks and K&S coverage (Security Work Tasks Covered, Occupational And Technical Knowledge And Skills Covered), Conditions, and Proficiency Standards. The work tasks and OTKS are summarized in Tables 19 and 20. Note that Table 20 is abbreviated for illustrative purposes.

Training Objectives for Personnel Security CWF1

Title:
Personnel Security CWF1—Define Personnel Security Standards

Scope:
CWF1 and its subordinate Tasks, Subtasks, and Knowledge and Skills

Prerequisites:
None. This training is for entry-level trainees in the Personnel Security discipline and related disciplines who need to obtain the basic knowledge and skills in CWF1.

Security Work Tasks Covered (Table 19):
Delineating Employment and Associational Requirements
Applying National Security Clearance and/or Specialized Access Requirements
Applying Reliability and/or Suitability Concerns

Occupational and Technical Knowledge and Skills Covered
See Table 20.

Conditions:
Refer to documentation and tools listed in Table 20.

Proficiency Standards:
At the conclusion of training, trainees will be able to demonstrate competence to meet the general performance, task knowledge, task performance, and OTKS complexity standards listed below:

- General Performance Standard: (1) work as team members, (2) perform task-level work competently, and (3) require major supervision
- KA Knowledge Standard: nomenclature and procedures
- KA Performance Standard: partial
- OTKS Complexity Standard: limited, basic, or working, as applicable

Table 19
Security Work Tasks, Subtasks, and Standards

Tasks	Subtasks (Performance Indicators)	Required Knowledge Levels	Required Performance Levels
1. Delineate Employment and Associational Requirements	• Identify, define, and monitor "employment" security standards • Identify, define, and monitor third-party contractor security standards • Identify, review, and monitor legal and regulatory constraints, if any • Develop program plans and/or processing requirements	B-procedures A-nomenclature	2-partial
2. Apply National Security Clearance and/or Specialized Access Requirements	• Identify, define, and monitor requirements and/or "specialized access" provisions • Identify and develop program objectives and processes • Identify, review, and monitor legal and regulatory constraints • Develop program plans and/or processing requirements	B-procedures A-nomenclature	2-partial
3. Apply Reliability and/or Suitability Concerns	• Identify, define, and monitor high risk task elements requiring greater reliability and/or suitability concerns • Participate in the determination and evaluation of job sensitivity designations • Identify, define, and monitor program objectives and processes • Identify, review, and monitor legal and regulatory constraints, if any • Develop program plans and/or processing requirements	B-procedures A-nomenclature	2-partial

Table 20
Required Occupational and Technical Knowledge & Skills and Standards[18]

Occupational and Technical K&S	Complexity Level
1. Policies, regulations, guidelines and ethical standards that govern the conduct of Personnel Security Investigations (including, but not limited to): • Investigative standards • Section 1001 and 1905, Title XVIII US Code and other applicable laws • DCID 6/4 • EO 12968 • EO 10450 • Privacy Act 1974 & Freedom of Information Act • Ethical standards (prohibitions and forbidden topics) • Other policies and directives	2-basic 1-limited
2. Adjudicative guidelines • Allegiance to the United States • Foreign influence • Foreign preference • Sexual Behavior • Personal Conduct • Financial considerations • Alcohol consumption • Drug involvement • Emotional, mental, personality disorders • Criminal conduct • Security violations • Outside activities • Misuse of information technology systems	1-limited
3. Investigation concepts, principles, and practices (including, but not limited to): • Types of investigations • Scope of investigations • Coverage requirements for each type of investigation (e.g., Single Scope Background Investigations (SSBI) and SSBI-Periodic Reinvestigations)	1-limited
4. Case and time management strategies	2-basic 1-limited
5. Information elicitation techniques (including, but not limited to): • Policies regarding telephonic interviews • Handling requests for presence of representation during interviews	2-basic 1-limited
12. Concepts, principles, and practices associated with the application of adjudicative criteria, disqualifying factors, and mitigating factors	1-limited
13. Agency-specific terminology, structure, instructions, correspondence procedures, or regulations	1-limited
14. Levels of clearance and access	3-working 2-basic 1-limited

APPLICATION 2. TRAINING ASSESSMENT

Training Assessment is the process of assessing training that already exists to determine what it covers (and does not cover). Various end-users might want to assess training for different reasons. For example, a manager or supervisor might assess several different types of training courses and media to determine what could be used to train employees. A training manager, developer, or trainer might assess a particular training course to determine how adequately it covers its subject and identify gaps that need to be filled to improve the course. The analysis

[18] This table is for illustrative purposes only and does not list all applicable OTKS.

may also determine depth of coverage and other properties of training. The product of a training assessment will typically be a matrix that shows what training does and does not cover. Skill standards provide an inventory of CWFs, KAs, and PIs performed on the job and the worker K&S required for competent performance. Training can be assessed by comparing its content with the content of some or all of the skill standards. Note that “training assessment” does not address training effectiveness because it does not measure the effects of training upon actual performance. It does, however, indicate whether training has the right ingredients to be effective.

Narrowing the Focus

Narrowing the focus in a training assessment depends upon the end-user’s objective and resources. If it is to survey a broad range of training options for several different security disciplines, then the focus needs to encompass all those disciplines and probably all seniority levels. If the objective is to review training options for a particular discipline and seniority level, then it is narrower. Assume for the sake of discussion that a training manager wants to determine what training is suitable for personnel security practitioners at entry, journeyman, and senior levels. The complete set of skill standards for personnel security is contained in Appendix G. These standards cover all work performed and K&S needed for workers at all seniority levels. The standards of greatest interest are 1 (Taxonomy), 2 and 3 (KA Knowledge and performance levels), and 5 (OTKS complexity). Standard 4 (A&E K&S) is excluded because it reflects academic and general workplace proficiencies rather than technical ones and would probably not be covered in introductory training. (See footnote 17 concerning possible applicability of A&E K&S.)

Data Sources

Data sources for a training assessment are existing training in its various forms, as well as other ways of obtaining information about training, such as the following:

- Reviewing course curricula and programs of instruction
- Reviewing published training objectives
- Reviewing course descriptions
- Reviewing test content
- Interviewing trainers and training developers
- Observing training
- Interviewing trainees
- Participating in training

Obviously, these data sources vary in cost and in the type of data they are likely to yield. The least costly are based on published information (e.g., curricula, training objectives, course descriptions, tests) and the most costly are based on active involvement in training (e.g., observing or participating in training, interviewing trainees). Interviewing trainers and training developers is somewhere in between these extremes, and is generally a good practice as a way of validating a document-based assessment. Ultimately, the end-user must decide what will work best within the resource constraints.

Application Tools

Application tools for training assessments are typically checklists, that is, lists with a box, scale, or other device attached to each list item. They are used to conduct an inventory and determine what is present and absent and possibly a scale value. Training Assessment checklists list training attributes to consider when reviewing existing training. These can be developed with different degrees of detail, depending upon the end-user's objectives and resources. For example, one might develop tools to check for the presence or absence of various combinations of KAs; KAs and PIs; KAs, PIs, and related knowledge and performance level scales; OTKS; and OTKS and related complexity scales.

Probably the simplest useful tool would be a KA checklist (a CWF checklist is possible but would be of questionable value) and, in fact, Tippit, Askia, Sepulveda, and Raasch (2005) recently used such a tool to assess a broad range of security training. It is simply a table that shows what KAs are covered in each training course with an "X" in the appropriate cells.

One JSTC contractor developed and applied a somewhat more detailed tool that covers KAs, PIs, and OTKSs. This is similar to the tool just described but has additional rows for OTKSs.

The format of a fragment of a hypothetical multidimensional tool is illustrated in Figure 2. This tool shows everything one might reasonably include in an assessment checklist and probably more than most end-users would want. To use this for training assessment, end-users would need to:

- Review each KA row separately and:
    - check off each KA covered
    - check off each PI covered
    - check off the knowledge levels covered
    - check off the performance levels covered

KAs Covered	PIs Covered	Knowledge Levels Covered	Performance Levels Covered
1. Delineate Employment and Associational Requirements	Identify, define, and monitor “employment” security standards Identify, define, and monitor third-party contractor security standards Identify, review, and monitor legal and regulatory constraints, if any Develop program plans and/or processing requirements	5-expert 4-advanced 3-working 2-basic 1-limited	4-highly proficient 3-competent 2- partially proficient 1- extremely limited
2. Apply National Security Clearance and/or Specialized Access Requirements	Identify, define, and monitor requirements and/or “specialized access” provisions Identify and develop program objectives and processes Identify, review, and monitor legal and regulatory constraints Develop program plans and/or processing requirements	5-expert 4-advanced 3-working 2-basic 1-limited	4-highly proficient 3-competent 2- partially proficient 1- extremely limited

OTKS Covered	Complexity Levels Covered
□ 1. Policies, regulations, guidelines and ethical standards that govern the conduct of Personnel Security Investigations (including, but not limited to): • Investigative standards • Section 1001 and 1905, Title XVIII US Code and other applicable laws • DCID 6/4 • EO 12968 • EO 10450 • Privacy Act 1974 & Freedom of Information Act • Ethical standards (prohibitions and forbidden topics) • Other policies and directives	5-expert 4-advanced 3-working 2-basic 1-limited
□ 2. Adjudicative guidelines • Allegiance to the United States • Foreign influence • Foreign preference • Sexual behavior • Personal conduct • Financial considerations • Alcohol consumption • Drug involvement • Emotional, mental, personality disorders • Criminal conduct • Security violations • Outside activities • Misuse of information technology systems	5-expert 4-advanced 3-working 2-basic 1-limited

Figure 2 Format of a Portion of a Hypothetical Instrument To Support the Training Assessment Application

- Review each OTKS row separately and:

- check off each OTKS covered
- check off the complexity levels covered

While completing a checklist sounds simple, in practice it may quite difficult, particularly if proficiency scales are involved. End-users may or may not be competent to make the necessary judgments and, if they are not, will have to obtain assistance from SMEs. Alternatively, one might couple the checklist with set of instructions so that it could be completed by SMEs.

APPLICATION 3. PERFORMANCE EVALUATION[19]

Performance Evaluation is the process of evaluating how well workers perform the job. The most common type of performance evaluation is the performance rating. Ratings are scaled proficiency estimates, typically made by a supervisor, based on current or previous observations of the person being evaluated. Performance tests are also scaled proficiency estimates, but made by an observer as the person being evaluated performs a task.

It is important to note that performance evaluations focus on actual performance, as demonstrated by observable behaviors. As such, they exclude the nonobservable, for example, what K&S workers are believed to possess.[20]

Skill standards can be used to develop both ratings and tests. In both cases, the evaluation consists of performance elements (e.g., KAs) with checklists and performance ratings attached to each element. The product of a performance evaluation is a set of ratings or test scores that estimates the testee's level of competence on certain dimensions of performance. Skill standards provide an inventory of CWFs, KAs, and PIs performed on the job and the worker K&S required for competent performance. Performance evaluation focuses on work performance using certain scales (see Table 15) that can be adapted for use in ratings and tests. The following discussion deals with performance ratings. Performance tests are used less often, are more difficult to develop and conduct, and are best left to professionals with testing expertise (e.g., educators, psychologists, test developers). Performance tests are seldom used in the workplace but most employees are familiar with performance ratings such as those used in the federal government to rate performance on a five-point scale (1-unacceptable, 2-minimally acceptable, 3-fully acceptable, 4-fully successful, 5-exceptional).

[19] Performance Evaluation is a "high stakes" application and has significant legal implications. See the cautionary notes at the beginning of this section.

[20] One might be able test for a nonobservable K&S with a performance test by designing a special task that requires the worker to apply the K&S in an observable way, but doing this is beyond the scope of this discussion.

Narrowing the Focus

Narrowing the focus in a performance evaluation depends upon whom the evaluator needs to evaluate and what performance dimensions are of interest. Assume for the sake of discussion that one needs to evaluate worker performance in the workplace setting, on a small set of technical tasks and subtasks (KAs and PIs), in the personnel security discipline, with workers at various seniority levels. This focus excludes nontechnical tasks such as those involving supervision, leadership, and management. The complete set of skill standards for personnel security is contained in Appendix G. These standards cover all work performed and K&S needed for workers at all seniority levels. The standards of greatest interest are 1 (Taxonomy) and 3 (KA performance levels). Standards 2 (KA knowledge levels) and 5 (OTKS complexity) are excluded because they are non-observable, and 4 (A&E K&S importance) because it deals with nontechnical tasks.[21] Skill standards 1 and 3 provide information that can be used to develop several rating scales, as described below.

Rating Scales

Rating scales can be adapted from the proficiency scales in Table 15 for Skill Standards 1 and 3. First, note that the three-level proficiency scale for Standard 1 at each level has three dimensions relating to Work Level, Worker Independence, and Leadership/Supervisory Role. Table 21 illustrates this three-level breakdown. For example, the Work Level dimension at entry level is to perform task-level work; at journeyman level, project-level work; and at senior level, system-level work.

Table 21
Breakdown of Skill Standard 1 Proficiency Scale Elements into Three Dimensions (Work Level, Independence, and Leadership/Supervisory Role)

Rating Dimension	Seniority Level		
	Entry	Journeyman	Senior
Work Level	Performs task-level work (associated with key activities) competently	Performs function- or project-level work at full performance level	Performs work at the system-level
Independence	Works as a team member	Works independently	Serves the role as technical subject-matter expert
Leadership /Supervisory Role	Requires major supervision	Mentors entry-level individuals	Directs technical work of others

Skill Standard 3 has a four-level proficiency scale with two dimensions relating to Completeness and Need for Help, as illustrated in Table 22.

[21] A&E K&S can and often are used in performance ratings but are excluded here because the focus is on technical tasks. Many employees are rated on such K&S, particularly if they are supervisors or managers.

Table 22
Breakdown of Skill Standard 3 Proficiency Scale Elements into Two Dimensions (Completeness, Need for Help)

Rating Dimension	Performance Level			
	1- extremely limited	2- partially proficient	3-competent	4-highly proficient
Completeness	Able to perform simple parts of the KA	Able to perform most parts of KA	Able to do all parts of the KA	Able to complete the KA quickly and accurately
Need for Help	Needs to be told or shown how to do most of the KA	Needs only help on hardest parts	Needs only a spot check of completed work	Can tell or show others how to do the KA

Note that Table 21 has a three-level scale and Table 22 has a four-level scale. Table 10 shows that the typical proficiency of entry-level workers on Skill Standard 3 starts at level 2 (partially proficient) rather than level 1 (extremely limited), which implies that it is possible for workers to perform at level 1 if they have sub-entry-level skill.

Table 23 merges the contents of Tables 21 and 22 with the changes just discussed. The Leadership/Supervisory Role dimension is nontechnical and can be excluded because of the earlier decision to focus exclusively on technical tasks. These are important dimensions for more senior workers, and would probably be included in a rating form designed to assess supervisory or leadership performance. The remaining four dimensions are both task related and observable.

Data Sources

Data sources for a performance evaluation are the rater's direct observation of performance or, alternatively, memory-based judgment of worker performance as observed at some time in the recent past.

Rating Form

Figure 3 is a set of instructions and a hypothetical rating form for KAs in the personnel security discipline. It is based on the contents of Table 23 but with some of the dimensions collapsed, the nontechnical ones deleted, and slight rewording. The form is essentially a checklist that allows the user to judge three separate dimensions of each KA (Worker Independence and Need for Help, Work Completeness, Working Level), on a 1-4 scale, under the conditions specified.

Table 23
Merged Contents of Five Rating Dimensions in Tables 16 and 17 with a Four-Level Rating Scale

Rating Dimension	Performance Level			
	1- extremely limited	**2- partially proficient**	**3-competent**	**4-highly proficient**
Completeness	Able to perform simple parts of the KA	Able to perform most parts of KA	Able to do all parts of the KA	Able to complete the KA quickly and accurately
Need for Help	Needs to be told or shown how to do most of the KA	Needs only help on hardest parts	Needs only a spot check of completed work	Can tell or show others how to do the KA
Work Level	Learning to perform task level work	Performs task-level work (associated with key activities) competently	Performs function- or project-level work at full performance level	Performs work at the system-level
Independence	Learning to work as team member	Work as a team member	Works independently	Serves the role as technical subject-matter expert
Leadership /Supervisory Role	Requires major supervision	Requires major supervision	Mentors entry-level individuals	Directs technical work of others

Instructions

Overview:

Your task is to rate worker job performance on each Key Activity on three performance dimensions (Worker Independence and Need for Help, Work Completeness, and Working Level). Each dimension is separate. Do not let the rating you give on any one dimension influence your other ratings.

How to Make Your Ratings:

1. Review Key Activity 1 and its Performance Indicators
2. Review the Worker Independence and Need for Help scale.
3. Check the box of the single statement that you believe most accurately describes the worker's Work Independence and Need for Help.
4. Review the Work Completeness scale.
5. Check the box of the single statement that you believe most accurately describes the worker's highest Work Completeness performance.
6. Review the Working Level scale.
7. Check the box of the single statement that you believe most accurately describes the worker's highest Working Level performance.
8. Repeat Steps 1-7 for the remaining Key Activities on the rating form.

Key Activity and Related Performance Indicators	**Rating Dimension**	**Performance Rating Scale**			
		1	**2**	**3**	**4**
KA1: Delineates Employment and Associational Requirements • Identifies, defines, and monitors "employment" security standards • Identifies, defines, and monitors third-party contractor security standards • Identifies, reviews, and monitors legal and regulatory constraints, if any • Develops program plans and/or processing requirements	Worker Independence and Need for Help (Check one)	Is unable to perform any part of the KA without help and requires major supervision	Is able to perform some parts of the KA but needs help on the hardest parts and requires major supervision	Is able to perform all parts of the KA independently without help	Is able to perform all parts of the KA independently and show others how to perform it
	Work Completeness (Check one)	Is able to perform simple parts of the KA	Is able to perform most parts of the KA	Is able to do all parts of the KA	Is able to complete the KA quickly and accurately
	Working Level (Check one)	Is not yet able to perform task-level work	Performs task-level work competently	Performs function- or project-level work at full performance level	Performs work at the system-level
KA2					
KA3					
etc.					

Figure 3 Format of a Portion of a Hypothetical Performance Rating Form to Support the Performance Evaluation Application

APPLICATION 4. JOB DEFINITION[22]

Job Definition is the process of defining a particular type of job. Its product is a job description or specification. Job descriptions tell what workers do on the job and may also include information about worker K&S. They may be used to define the necessary qualifications of workers; advertise job openings and hire new workers or promote or reassign job incumbents; standardize work in a particular security discipline or type of job; write contractual statements of work; and in various other ways. Job descriptions come in various forms, but typically include some combination of the following elements:

- Work functional areas
- Scope of responsibilities
- Technical duties and tasks
- Leadership, management, and supervisorial responsibilities, if applicable
- Technical K&S
- General workplace and academic K&S
- Description of the work environment

Skill standards cover much of this territory and can be very useful in writing job descriptions. Job descriptions intended for use in hiring, promotion, or reassignment typically include all of these elements because they need to describe both the work and the necessary K&S of prospective employees. Descriptions of the work itself (as in position descriptions) do not necessarily have to include information about worker K&S.

Narrowing the Focus

Assume for the sake of discussion that an employer wants to write a job description for the purpose of hiring a journeyman-level worker to perform personnel security work of a technical, nonsupervisorial, nonmanagerial nature. The complete set of skill standards for personnel security is contained in Appendix G. These standards cover all work performed and K&S needed for workers at all seniority levels. Let us narrow the focus by concentrating only on CWFs 1 and 2. All five skill standards contain information that is relevant in composing a job description that might be used to publicize a work position available for hiring.

Composing a Job Description

Let us compose a job description step by step with the elements listed above.

[22] Job Definition may be a “high stakes” application if it affects personnel decisions such as hiring, promotion, or job assignment. See the cautionary notes at the beginning of this section.

Work Functional Areas. These comprise CWF1 (Define Personnel Security Standards) and CWF2 (Define Additional Vendor and Contractor Standards). They may be combined and restated as, *Defines Personnel Security Standards and Standards for Vendors and Contractors.*

Scope of Responsibilities. The job description is for a journeyman-level worker to perform personnel security work of a technical, nonsupervisory, nonmanagerial nature and an applicable scope of responsibilities statement is the following, Technical, nonsupervisory, nonmanagement. Job incumbent performs technical duties and tasks and assists others and may serve as a role model or mentor for other job incumbents.

Technical Duties and Tasks. Arguably, the most important part of a job description is to define the relevant duties and tasks, which correspond to Key Activities and Performance Indicators in the skill standards. The usual convention is write duty and task statements in the active voice. Personnel Security KA1 and its PIs can be condensed and rewritten as duty and task statements by simply adopting different terminology and rewriting the PIs as active-voice tasks. For example, here is a duty and task statement based on KA1:

1. <u>Delineates Employment and Associational Requirements:</u> Identifies, defines, and monitors “Employment” security standards and third-party contractor security standards. Identifies, reviews, and monitors legal and regulatory constraints, if any. Develops program plans and/or processing requirements.

Technical K&S. Technical K&S correspond to OTKS in the skill standards. The OTKS could be used directly but, as a practical matter, a job description probably does not need to be this detailed. Many of the OTKS contain a header and subordinate bulleted items and it is sufficient to list the header alone. For example, here are three Technical K&S based on the first three OTKS:

1. Policies, regulations, guidelines and ethical standards that govern the conduct of Personnel Security Investigations

2. Adjudicative guidelines

3. Investigation concepts, principles, and practices

General Workplace K&S. General Workplace K&S is a more common term for A&E K&S in the skill standards. Some or possibly all of these may be of importance to varying degrees in a job description, particularly if the description is being used to inform potential employees about necessary qualifications for a job opening. These general workplace K&S may be presented in simple laundry list fashion, although it would be more useful to most readers if they were prioritized in order of importance with additional remarks about how they apply on the job.

Example of a Job Description

The following pages present an example of a job description based on the framework described above. The description should be self-explanatory.

JOB DESCRIPTION

Journeyman-Level Personnel Security Specialist

Work Functional Areas:

Defines Personnel Security Standards and Standards for Vendors and Contractors

Scope of Responsibilities:

Technical, nonsupervisory, nonmanagement. Job incumbent performs technical duties and tasks and assists others and may serve as a role model or mentor for other job incumbents.

Technical Duties and Tasks:

1. <u>Delineates Employment and Associational Requirements:</u> Identifies, defines, and monitors “Employment” security standards and third-party contractor security standards. Identifies, reviews, and monitors legal and regulatory constraints, if any. Develops program plans and/or processing requirements.

2. <u>Applies National Security Clearance and/or Specialized Access Requirements:</u> Identifies, defines, and monitors requirements and/or “specialized access” provisions. Identifies and develops program objectives and processes. Identifies, reviews, and monitors legal and regulatory constraints, if any. Develops program plans and/or processing requirements.

3. <u>Applies Reliability and/or Suitability Concerns:</u> Identifies, defines, and monitors high-risk task elements requiring greater reliability and/or suitability concerns. Participates in the determination and evaluation of job sensitivity designations. Identifies, defines, and monitors program objectives and processes. Identifies, reviews, and monitors legal and regulatory constraints, if any. Develops program plans and/or processing requirements.

4. Applies Qualification and Reliability Standards: Determines qualification and reliability standards. Identifies sources of relevant information. Identifies, reviews, and monitors legal and regulatory constraints, if any. Develops system to collect and evaluate necessary information. Defines process to make determination and process to document and notify appropriate responsible authorities.

5. Verifies Applicable Conditions of Association: Determines conditions of association that require verification. Defines dissemination requirements. Determines most efficient way of verification. Determines most efficient way to disseminate information.

6. Monitors Conditions of Contractor Standards: Determines elements of contractor standards that require monitoring. Determines restrictions on monitoring by affected organizations. Evaluates self-reporting processes. Defines documentation and dissemination requirements.

Job Incumbent Minimum Required Knowledge and Performance Levels:

1. Knowledge Level: Knowledge of nomenclature, procedures, and principles relating to personnel security standards. Must know appropriate terminology, procedures, and why and when each duty must be performed.

2. Performance Level: Fully competent to perform each duty independently with minimal supervision.

Job Incumbent Minimum Required Job-Specific Knowledge and Skills. Incumbent must be able to independently apply the knowledge and skills listed below across a range of duties and tasks to meet typical work requirements and having moderate consequences for error (roughly equivalent to the level typically attained through multiple training courses or a two-year or technical school degree, or 6–24 months of direct application or use of this knowledge or skill):

1. Policies, regulations, guidelines and ethical standards that govern the conduct of Personnel Security Investigations

2. Adjudicative guidelines

3. Investigation concepts, principles, and practices

4. Case and time management strategies

5. Information elicitation techniques

6. Concepts, principles, and practices associated with the application of adjudicative criteria, disqualifying factors, and mitigating factors

7. Agency-specific terminology, structure, instructions, correspondence procedures, or regulations

8. Levels of clearance and access
9. Interim access criteria and justifications
10. Terminologies
11. Special Program case procedures
12. Physical security requirements associated with personnel security
13. Computer and information systems usage guidelines
14. Concepts and principles of clearance, access, reliability, suitability, and trustworthiness
15. Ethical issues associated with personnel security
16. Third party release provisions
17. Risk management concepts, principles, and practices
18. Record management requirements as related to personnel security
19. Information Assurance requirements as related to personnel security
20. Information System Security requirements as related to personnel security
21. Operations Security Program requirements as related to personnel security
22. Personnel security-related funding, manpower requirements, and budgeting programs
23. Personnel security regulations and processes including protected information status, determination, assessment procedures, security, marking, control, accountability, and safeguarding of records
24. Preparation, coordination, and execution of MOU, MOA, Interservice Support Agreements, and Service Level Agreements
25. Program evaluation concepts, methods, and techniques
26. National disclosure policies
27. Development, preparation, and execution of personnel security plans
28. Development, preparation, and execution of personnel security policies and procedures
29. Methods for analyzing, organizing, compiling, and reporting personnel security data

Job Incumbent Minimum Required General Workplace and Academic Knowledge and Skills. Incumbents must be able to independently apply the knowledge and skills listed below across a range of duties and tasks to meet typical work requirements and having moderate consequences for error:

- Analyzing and Solving Problems—Anticipate or identify problems and their causes; develop and analyze potential solutions or improvements using rational and logical processes or innovations and creative approaches when needed.
- Gathering and Analyzing Information—Obtain facts, information or data relevant to a particular problem, question or idea through observation of events or situations, discussions with others, or research or retrieval from written or electronic sources; organize, integrate, analyze and evaluate information.
- Making Decisions and Judgments—Make decisions that consider relevant facts and information, potential risks and benefits, and short- and long-term consequences or alternatives.
- Organizing and Planning—Organize and structure work for effective performance and goal attainment; set and balance priorities; anticipate obstacles; formulate plans consistent with available human, financial, and physical resources; modify plans or adjust priorities given changing goals or conditions.
- Using Information and Communications Technology—Select, access and use necessary information, data, and communications-related technologies, such as basic personal computer applications, telecommunications equipment, Internet, electronic calculators, voice mail, email, facsimile machines and copying equipment to accomplish work activities.
- Working in Teams—Work cooperatively and collaboratively with others to achieve goals by sharing or integrating ideas, knowledge, skills, information, support, resources, responsibility and recognition.
- Writing—Express ideas and information in written form clearly, succinctly, accurately, and in an organized manner; use English language conventions or spelling, punctuation, grammar, and sentence and paragraph structure; and tailor written communication to the intended purpose and audience.

Work Environment:

Work is performed in an office setting.

APPLICATION 5. CERTIFICATION[23]

Please note that this subsection refers to the earlier subsections on *Training Definition*, *Training Assessment*, and *Performance Evaluation.* It is important to understand the contents of those subsections before reading what follows.

[23] Certification is a “high stakes” application and has significant legal implications. See the cautionary notes at the beginning of this section.

Certification is the process of determining whether or not a worker is able to meet criteria and standards required at a particular seniority level. Certifications come in various forms and are awarded by many different bodies (e.g., agencies, schools, professional societies); range from narrow to broad (e.g., in a single skill or task to a trade or profession); are qualified for in such ways as completing training or job assignments, prior work experience, and demonstrating proficiency on a test; and vary in other ways as well.[24] All certifications require candidates to satisfy criteria and standards set by a certifying authority. Skill standards can be useful in setting some of these criteria and standards.

Profession, Discipline, and Skill Certifications

It is useful to distinguish among certifications at the profession, discipline, and skill levels, as they tend to differ in predictable ways. Profession certifications are usually awarded by certifying bodies such as professional societies to senior practitioners in positions of influence or leadership based upon evidence of career accomplishments, experience, and education, and are broad in scope. Discipline-based certifications are usually awarded by such bodies as schools or agencies to journeyman or senior practitioners who perform technical (versus supervisory or management) work based upon evidence of completion of education and training, job assignments, work experience, and demonstrated work proficiency. Skill-based certifications are similar to discipline-based but narrower in scope and analogous to military job skills proficiency qualifications; a worker may hold several such certifications based upon completion of training courses, job assignments, work experience, satisfactory performance on qualifying tests, etc. Probably the two most common forms of skill certifications are training-based and test-based certifications.

Certification Programs

Certification normally occurs within a formal certification program that has certification criteria, standards, and procedures for assessing candidate certification eligibility. Certification programs work by defining the certification criteria, setting certification standards, assessing candidate qualifications against the criteria and standards, and certifying qualified candidates and not certifying the unqualified.

Legal Considerations

Certification programs must often address legal issues to avoid possible legal challenges by certification candidates. For example, one important issue is the validity of tests or other procedures used to measure applicant competence.

[24] Some certifications involve credentialing or licensing , may influence personnel decisions (e.g., hiring, promotion, job assignments), and have significant legal implications. Others focus on professional development and do not affect personnel decisions or have legal implications.

Personnel may take legal action against an employer who makes personnel decisions (e.g., hiring, promotion, job assignments) based on questionable certification criteria, standards, or procedures. Assuring validity has legal ramifications but is a technical matter that usually requires professional expertise in competence assessment (e.g., testing, measurement, statistics). Agencies developing certification programs should assure that their program development team include persons with the necessary expertise.

Another possible legal issue is that agencies conducting their own programs may be required to provide employees with the necessary resources and training to meet certification requirements and assure that training is effective and does not require employees to perform duties or functions that may create liabilities (Simpson, Fischer, Tippit, Rizzoli, & Denk, 2004). These issues are beyond the scope of current discussion, but those who plan to implement certification programs should research them fully and consult legal counsel before proceeding.

Certification Criteria and Standards

Certification criteria vary with the particular program and type of certification. Several such criteria were mentioned above (e.g., professional standing, career accomplishments, experience, education, training, job assignments, work experience, demonstrated proficiency, and test performance). Any of these criteria relating to work performance and job-related K&S link directly to the skill standards. For example, work-related technical training, job assignments, experience, and test performance all have this link. Criteria that do not relate to work performance or K&S have little or no relation to the skill standards. Examples of unrelated criteria are professional standing, career accomplishments, and general educational attainments.

Setting Certification Criteria and Standards. Certification standards are the benchmarks that certification candidates must meet on each of the certification criteria.

Together, certification criteria and standards address these questions:

- What should a certified worker be able to do?
- How well should he or she be able to do it?
- What K&S should the worker possess?[25]

Note that these questions closely parallel those addressed in the *Training Definition* application. The product of that application is a set of training objectives that defines what trainees should be able to do after training in terms specific tasks, conditions, and standards. The objectives were developed by (1) narrowing the focus

[25] The K&S may include any combination of the technical (i.e., OTKS) and nontechnical (i.e., A&E K&S) acquired through training, job assignments, work experience, and in other ways.

to specific KAs and one seniority level, (2) deciding what skill standards to cover in training, and (3) developing the corresponding training objectives. In developing certification criteria and standards, the first two steps are identical, and Step 3 becomes *identify the certification criteria and standards*.

Despite the parallel between Training Definition and Certification, there are some important differences. First, training is most often defined for entry-level workers, although certification programs are usually developed for journeyman or senior workers. Second, A&E K&S, which were excluded from consideration in Training Definition, may be relevant in Certification, particularly for senior-level certification candidates. For example, a certification program might very well treat A&E K&S such as adaptability, building consensus, leading others, organizing and planning, speaking, writing, and use of interpersonal skills as important criteria for certification.

Assessing Certification Candidates. A certification program must have a way to assess candidate qualifications against the certification criteria and standards. Several types of qualifying evidence were mentioned above (e.g., completion of education and training, job assignments, work experience, demonstrated work or test proficiency). The evidence may be provided in several different forms (e.g., training certificates, work records, written statements from supervisors, performance ratings, knowledge testing). The skill standards may be used to set criteria and standards for the various forms of qualifying evidence. To illustrate this more concretely, let us consider three criteria commonly used in Discipline and Skill-based certification programs: (1) completion of training, (2) performance evaluation, and (3) knowledge testing.

A program may certify based on *completion of training* if (1) the training covers subjects in the depth required by the certification criteria and standards, (2) the training is effective in accomplishing training objectives, and (3) ex-trainees provide evidence of successful completion. On the first point—training coverage and depth—the *Training Assessment* subsection described how to use skill standards to determine training coverage, depth, and other properties. On the second point—training effectiveness—the skill standards are not directly helpful.[26] As a practical matter, the certifying authority must usually make this judgment based on the preponderance of evidence in whatever form it is available (e.g., expert opinion, course reputation, performance of former students). On the third point, credible evidence is whatever the certifying authority decides it is (e.g., certificate, diploma, test score).

[26] Training effectiveness assessment is a complex matter and well beyond the scope of this discussion. In practice, it is most commonly based on subjective measures, such as opinions of managers and ratings by former trainees, rather than objective outcome measures such as training transfer to the workplace. One important consideration is how training determines trainee learning and performance levels after training, if at all.

A program may certify based on *performance evaluation* with performance tests or ratings as discussed earlier in the *Performance Evaluation* subsection. That discussion illustrated how to develop a performance evaluation rating form (Figure 3) that could be used by a supervisor in the workplace, but it also applies more generally to any type of performance rating given in any context, for example, in training, in a certification workshop, etc. Such ratings and performance tests could be used for certification.

A program may certify based on *knowledge testing* using written tests.[27] The skill standards suggest written knowledge test items in any of the common formats, such as multiple choice, fill-in the blank, true-false, open-ended, and so forth. The standard of greatest interest for developing test items is 5 (OTKS complexity). Skill standards 1 [Taxonomy] and 2 [KA knowledge levels] could also be used but are not as easily translatable into test items. For purposes of discussion, let us focus on Skill Standard 5. Before composing a test item based on the OTKS, note the following:

- The OTKS dictate test item topics by describing what K&S are required for competent performance.
- The OTKS usually lack sufficient detail alone for writing meaningful test items.
- Test items should be written by SMEs or with SME assistance.
- Test item information content must be based on a valid, verifiable source.

Table 24 shows five model multiple-choice test items that relate to Personnel Security OTKS 2, 14, 17, 27, and 37 (see Skill Standard G-4) and the sources used to generate their information content. The instructions paired with these items would tell test takers to select the single answer that is the most correct.

[27] Written tests are widely used in the private sector. Examples are physician board examinations, lawyer bar examinations, engineer professional examinations, CPA certification examinations for accountants, and security professional Certified Protection Professional (CPP) examinations administered by ASIS International.

Table 24
Selected Personnel Security OTKS with Model Multiple-Choice Test Items and Related Information Content Sources

OTKS	Test Item	Source
2. Adjudicative guidelines	Which of the following potentially disqualifying conditions or behaviors does <u>not</u> fall under the Personal Conduct adjudicative guideline for clearance eligibility: a. Association with persons involved in criminal activity. b. Deliberate omission of relevant material facts from a personnel security questionnaire. c. Sexual behavior that causes an individual to be vulnerable to coercion, exploitation or duress. d. A pattern of dishonesty or rule violations.	Adjudicative Desk Reference, PERSEREC
14. Levels of clearance and access	If an employee is adjudicated as eligible for access to Top Secret information, that individual can be given: a. Any classified information. b. Only Top Secret information. c. Sensitive Compartmented Information. d. Information up to and including Top Secret if that person has a legitimate need-to-know.	DoDD 5200.1-R, DoD Information Security Program
17. Special Program case procedures	Personnel security requirements for work in a special access program: a. Includes a clearance above Top Secret. b. May be more stringent that those for non-SAP classified programs. c. Must include access to Sensitive Compartmented Information (SCI). d. Do not include an appeal process following suspension of access.	DoD 5220.22-M-Sup 1, National Industrial Security Program Operating Manual Supplement
27. Risk management concepts, principles, and practices	The central premise of risk-management decision-making is that loss or compromise of classified or sensitive information: a. Must be avoided at all costs. b. Can be prevented only so far as budgets allow for spending on security. c. Can be effectively minimized by policy implementation governed by the levels of threat, vulnerability, consequence of loss, and criticality. d. Policy implementation must be uniform across federal agencies.	GAO-02-150T, Homeland Security, Key Elements of a Risk Management Approach
37. National disclosure policies	National Disclosure Policy permits the disclosure of U.S. classified information to a representative of a foreign country: a. Only by senior officials designated as Principal Disclosure Authorities or their delegated authorities. b. Only after Presidential authorization. c. By any federal employee with a Top Secret clearance. d. Only if that country has a bilateral security arrangement with the United States.	International Programs Security Handbook, DoD, OUSD(Policy)

DISCUSSION AND CONCLUSION

Tippit et al.'s 2002 baseline study was intended to build consensus on the architecture of the security profession and a common language and to define core security competencies at entry, journeyman, and senior levels. It provided the basis for accomplishing all of these objectives in the current project, which was conducted to vet the taxonomies, develop skill standards and application guidance, and document the method used. To our knowledge, this is the first time that skill standards have been developed for the seven security disciplines. The current report provides the resources and tools needed to achieve these objectives. The challenge now rests with security policymakers, leaders, and the security community itself to put the standards to work in practical applications. The applications in this report are intended as tools rather than as prescriptions, and readers are encouraged to modify them as needed based on their particular requirements.

As stated in the "cautionary notes" in the previous section, it is safe to regard the skill standards as a reasonable description of the work performed in each security discipline and the K&S that workers need to perform it competently, but it is also important to keep their limitations in mind. First, they describe disciplines, not jobs. Second, they are unvalidated through field surveys of job incumbents; conducting such surveys may be important in high-stakes applications such as certification and performance evaluation. Third, they describe the disciplines based on a snapshot in time representing roughly the year 2004. On the last point, security disciplines will certainly change in the future and end-users will need to modify the standards to reflect these changes as they occur.

Performing the applications requires relevant technical and professional background and experience and most require more than security subject-matter expertise. Some of the applications—such as performance evaluation and certification—have significant legal implications. Human resource and security professionals will be able to use the standards directly in many applications, but where applications may impact on employment-related decisions, are advised to seek assistance from legal counsel or professional experts if in doubt about how to proceed.

DISCUSSION AND CONCLUSION

REFERENCES

Brannick, M.T., & Levine, E.L. (2002). *Job analysis: Methods, research, and applications for human resource management in the new millennium*. Thousand Oaks, CA: Sage.

Butler, E.C. (1972). *Instructional systems development for vocational and technical training*. Englewood Cliffs, NJ: Educational Technology Publications.

Cascio, W.F. (1991). *Applied psychology in personnel management*. Englewood Cliffs, NJ: Prentice-Hall.

DoD Security Review Commission. (1985). *Keeping the nation's secrets: A report to the Secretary of Defense by the Commission to Review DoD Security Policies and Practices*. Washington, DC: Office of the Secretary of Defense.

Fischer, L.F. (2004). (FOUO) *Preferences and priorities for professional development programs: Management and executive perspectives on the security workforce (Interim Report)*. Monterey, CA: Defense Personnel Security Research Center.

General Accounting Office. (1994). *Management reform: Implementation of the national performance review's recommendations (GAO/OCG-95-1)*. Letter Report. Washington, DC: Author.

General Accounting Office. (1996a). *Information security: Opportunities for improved OMB oversight of agency practices* (GAO/AIMD-96-110). Washington, DC: Author.

General Accounting Office. (1996b). *Training: Opportunities exist to reduce the training infrastructure* (GAO/NSIAD-96-93) (Letter Report, 03/29/96). Washington, DC: Author.

General Accounting Office. (1996c). *Information security: Computer attacks at Department of Defense pose increasing risks* (GAO/AIMD-96-84). Washington, DC: Author.

General Accounting Office. (1999). *Information security risk assessment: Practices of leading organizations* (GAO/AIMD-99-139). Washington, DC: Author.

General Accounting Office. (2002a). *Nuclear security: Lessons to be learned from implementing NNSA's security enhancements* (GAO-02-358). Washington, DC: Author.

General Accounting Office. (2002b). *Homeland security: Information sharing activities face continued management challenges* (GAO-02-1122T) . Washington, DC: Author.

REFERENCES

Joint Security Commission. (1994). *Redefining security: A report to The Secretary of Defense and the Director of Center Intelligence*. Washington, DC: Department of Defense.

Joint Security Commission. (1999). *A report by the Joint Security Commission II, Phase I*. Washington, DC: Department of Defense.

Mager, R.F. (1962). *Preparing objectives for programmed instruction*. San Francisco: Fearon.

Mager, R.F. (1997). *Preparing instructional objectives: A critical tool in the development of effective instruction* (3rd. ed.). Atlanta, GA: Center for Effective Performance.

Marshall-Mies, J.C., & Fischer, L.F. (2003). *Preferences and priorities for professional development programs: Focus group perspectives on the security workforce* (Interim Report). Monterey, CA: Defense Personnel Security Research Center.

Marshall-Mies, J.C., Lupton, T.B., & Fischer, L.F. (2003). *Review of (ISC)2 training and certification programs to inform the development of a model for certifying security professionals*. (Interim Report). Monterey, CA: Defense Personnel Security Research Center.

McCormick, E.J. (1979). *Job analysis*. New York: Amacom.

Melching, W.H., & Borcher, S.D. (1973). *Procedures for constructing and using task inventories. Center for Vocational and Technical Education, Research and Development Series No. 91*. Columbus, Ohio: The Ohio State University. [quoted in McCormick]

Merriam-Webster. (1986). *Webster's ninth new collegiate dictionary*. Springfield, MA: Author.

National Skill Standards Board. (2000a). *Built to work: A common framework for skill standards*. Washington, DC: Author.

National Skill Standards Board. (2000b). *Skill scales companion guide*. Washington, DC: Author. Retrieved January 4, 2005, from http://www.tssb.org/wwwpages/SkillScalesCompanionGuide.pdf

National Skill Standards Board. (2002a). *Information and Communication Technology (ICT) work analysis plan*. Washington, DC: Author.

National Skill Standards Board. (2002b). *Using skill standards and certifications in workforce investment board programs*. Washington, DC: Author.

Simpson, H.K., Fischer, L.F., Tippit, J.D., Rizzoli, R., & Denk, R.P. (2004). *Development of training policy for security practitioners* (Management Report PERS-MR-04-6). Monterey, CA: Defense Personnel Security Research Center.

Tippit, J.D., & Askia, P.F. (2002). *A study of professional development programs.* Foster City, CA: The Tippit Group.

Tippit, J.D., Askia, P.F., Sepulveda, G., & Raasch, R. (2005). *Body of knowledge report.* Foster City, CA: The Tippit Group.

Tippit, J.D., & Rizzoli, R.A. (2001). *A study to define the Defense Security Service training mission as mandated by regulatory issuance and agreement* (Interim Report). Foster City, CA: The Tippit Group.

Tippit, J.D., & Rizzoli, R.A. (2003). *A study to define the intelligence community training mission as mandated by regulatory issuance and agreement* (Interim Report). Foster City, CA: The Tippit Group.

Tippit, J.D., Rizzoli, R.A., Denk, R.P., & Fischer, L.F. (2001). *Defining the DSS training mission* (Management Report PERS-MR-01-5). Monterey, CA: Defense Personnel Security Research Center.

Tippit, J.D., Rizzoli, R.A., Baker, S., & Miller, M.A. (2002). *Baseline definition of the security profession* (Interim Report). Foster City, CA: The Tippit Group.

U.S. Department of Labor. (2004). *Knowledge skills and abilities.* Retrieved January 11, 2005, from http://www.doleta.gov.

REFERENCES

APPENDIX A

BIBLIOGRAPHY OF SECURITY JOB-RELATED DOCUMENTATION REVIEWED BY TIPPIT et al. (2002)

BIBLIOGRAPHY OF SECURITY JOB-RELATED DOCUMENTATION REVIEWED BY TIPPIT ET AL. (2002)

American Society for Industrial Security. (2001). *Proceedings of the 2001 academic/practitioner symposium*. Washington, DC: Author.

Bintliff, R.L. (1992). *The complete manual of corporate and industrial security.* New York: Prentice-Hall.

Central Intelligence Agency, Office of Security. (2001). *Multi-disciplined security officer (MDSO) career development path.* Washington, DC: Author.

Central Intelligence Agency, Office of Security. (2001). *OS career tracks plan.* Washington, DC: Author.

Community Management Staff and U.S. Security Policy Board Staff. (2000). *Security training and professional development study*. Washington, DC: Author.

Crowe, T.D. (1991). *Crime prevention through environmental design.* Louisville, KY: National Crime Prevention Institute.

Cunningham, W.C., & Taylor, T.H. (1985). *Private security and police in America.* London: Butterworth-Heinemann.

Cunningham, W.C., Strauchs, J.S., & Van Meter, C.W. (1990). *Private security trends 1970-2000.* London: Butterworth-Heinemann.

Defense Acquisition University. (1997). *Technology-based education and training plan, concept document, version 2.01*. Washington, DC: Author.

Defense Systems Management College. (1998). *Defense systems management college research, consulting and information dissemination.* Ft. Belvoir, VA: Author.

Department of Energy. (1999). *Department of energy professional enhancement program*. Washington, DC: Author.

Fennelly, L.F. (Ed.). (1989). *Handbook of loss prevention and crime prevention (2nd. ed.).* London: Butterworth-Heinemann.

Fischer, R.J., & Green, G. (1998). *Introduction to security (6th. ed.*). London: Butterworth-Heinemann.

Healy, R.J., & Walsh, T.J. (2000). *Protection of assets manual, Vols. I-IV.* Santa Monica: Merritt Co.

Intelligence Community Officers Program, Brochure, Intelligence Community.

Kingsbury, A.A., & Post, R.S. (1974). *Security administration: An introduction, (2nd. ed.).* London: Butterworth-Heinemann.

Kingsbury, A.A., & Post, R.S. (1991). *Security administration: An introduction to the protective services (4th. ed.*). London: Butterworth-Heinemann.

Langer, S. (2001). *Compensation in the security/loss prevention field (parts 1 and 2) (13th ed.).* Abbott Langer & Associates Inc.

Marshall-Mies, J.C. (1987). *Determination of training requirements: Personnel security specialists (adjudicators).* HumRRO International.

McLaughlin, A. (1990). *Report of the president's commission on aviation security and terrorism.* Washington, DC: Author.

National Reconnaissance Office. (1999). *NRO competency modeling study, security competency model*. Washington, DC: Author.

Nonproliferation and National Security Institute. (2001). *Background information on government-wide human capital crisis*. Albuquerque, NM: Author.

Safeguards and Security Central Training Academy. (n.d.). *Diploma program guidelines*. Washington, DC: Author.

Shea, J. R. (1994). *Resource estimates for counterintelligence security and related activities.* Alexandria, VA: Institute for Defense Analyses.

Shea, J. R. (1996). *Resource estimates for information systems security.* Alexandria, VA: Institute for Defense Analyses.

Shea, J. R. (1998). *Security resources in the DoD infrastructure.* Alexandria, VA: Institute for Defense Analyses.

Shea, J. R. (1999). *Mission area analysis of DoD counterintelligence.* Alexandria, VA: Institute for Defense Analyses.

Shea, J. R. (2001). *Framework for a broad area review of protection policies, Vol. I: Main report.* Alexandria, VA: Institute for Defense Analyses.

Shea, J. R. (2001). *Framework for a broad area review of protection policies, Vol. II: Quantitative estimates of the security work force.* Alexandria, VA: Institute for Defense Analyses.

Timm, H.W., & Christian, K.E. (1991). *Introduction to private security*. Stamford, CT: Brooks/Cole.

U.S. Army Human Resources Command. (2001). *Army civilian training, education and development system (ACTEDS) plan for career program 35 (intelligence)(3rd. ed.).* Alexandria, VA: Author.

U.S. Department of Justice. (1995). *Vulnerability assessment of federal facilities*. Washington, DC: Author.

U.S. Security Policy Board. (2001). *Personnel security investigations training standards*. Washington, DC: Author.

APPENDIX B

WORKSHOP EXHIBITS

Exhibit B-1
Pre-Workshop Tasking Email Sent to SMEs for the Communications Security Workshop

Message subject line: Welcome to PERSEREC's Communications Security Workshop, 14-16 September in Monterey

Welcome in advance to PERSEREC's 14-16 September workshop in Monterey to define skill standards for Communications Security professionals. Participants in previous workshops—dealing with Physical, Information, and Personnel Security, Security Investigations, and Security Management—became very involved and made them all very successful.

The workshop will require three full days of fairly intense effort to achieve its goals. To assure that we get off to a quick start on the very first day, I request that you do two things before the workshop: (1) perform a pre-workshop task and (2) help identify and, if possible, obtain relevant Communications Security documentation, as described below.

Pre-Workshop Task

The PERSEREC research team recently produced a taxonomy describing Communications Security in terms of *Critical Work Functions* (major responsibilities of work). Each *Critical Work Function* is comprised of *Key Activities* (major duties or tasks), and *Key Activities* are comprised of *Performance Indicators* (subtasks). The taxonomy is attached in the form of an outline (*comsec taxonomy version 1.doc*).

The taxonomy will be used in the workshop. However, <u>before the workshop</u>, it needs a critical evaluation by experts, such as yourself, who have extensive work experience in the security profession. Please review the outline and try to answer these questions:

First, consider the top level in the outline. How well do these *Critical Work Functions* represent the scope of what Communications Security professionals do? Specifically, should any *Critical Work Function* be added, deleted, or changed?

- Next, consider the second level of the outline. How well do the *Key Activities* listed for each *Critical Work Function* represent its scope? Specifically, should any *Key Activities* be: added, deleted, changed, or reassigned to another *Critical Work Function*?
- Finally, consider the third level of the outline. How well do the *Performance Indicators* listed for each *Key Activity* represent its scope? Specifically, should any *Performance Indicators* be: added, deleted, changed, or reassigned to another *Key Activity*?

You may provide your changes and comments in any of the following ways:

- Edit or insert them directly in the taxonomy and email to simpsohk@osd.pentagon.mil. (You may find it easier to view and edit by selecting the *Outline* option on the *View* menu.)
- Email or FAX them separately (FAX: 831-657-0153 - Attn: Henry Simpson)

Please send us your changes and comments <u>on or before 10 September</u>. This will give us enough time to copy them so that you may present them to the group on the first day of the workshop.

Exhibit B-1 Cont.

Call for Communications Security Documentation

Please help us identify and obtain any documents describing Communications Security job functions, duties, tasks, skills, knowledge, competencies, or other job-related information. The following types of documentation would be very helpful:

1. Previous job-task and skill standards analyses
2. Course curricula and plans of instruction (POIs)
3. Instructional Systems Development and other course development documentation
4. Published training objectives (enabling and terminal) and course descriptions
5. Performance standards used by Federal agencies
6. OPM position classification standards
7. Position descriptions used by Federal agencies
8. Professional development program documentation
9. Research reports on professional development and related questions

Please mail, email, or fax us a copy of whatever you identify as soon as possible so that we may copy it for the workshop. If there is not enough time to send it before the workshop, bring a copy with you to the workshop. The PERSEREC mailing address is:

Personnel Security Research Center
99 Pacific Avenue, Suite 455-E
Monterey, CA 93940
Attn: Henry Simpson

Recommended Background Reading

The Communications Security framework is based on the attached PERSEREC research study (*Definition of Security Profession.doc*). You may find it helpful to review the report for background and to see how it fits Communications Security within the total context of the Security Profession. John Tippit, the report’s principal author, will discuss the report on the first day of the workshop.

I hope that the taskings described in this email are clear. If they are not, or if you have any questions, contact me by phone (831-657-3056) or email (simpsohk@osd.pentagon.mil).

--Henry Simpson

Exhibit B-2
Names and Affiliations of Workshop SMEs for Each Security Discipline

Discipline	SME Names and Affiliations
Physical Security	Melvin E. Kerr, formerly with Defense Finance and Accounting Service and U.S. Air Force Carol A. Bolden, formerly with Defense Contract Management Administration Office Bob Copeland, Defense Advanced Research Projects Agency Richard Williams, formerly Director of Defense Security Programs, OSD and additional participants from the Naval Criminal Investigative Service, Defense Threat Reduction Agency, and The Tippit Group.
Information Security	Tom Bozek, formerly Director, Critical Infrastructure Protection Program Walter Davis, USAF Declassification Office Donja Stephenson, Naval Criminal Investigative Service Lloyd Taylor, formerly Senior Instructor, Department of Defense Security Institute Richard Williams, formerly Director of Defense Security Programs, OSD and additional participants from the Information Security Oversight Office and Defense Security Service Academy.
Personnel Security	Gybrilla Blakes, Defense Security Service Academy Donja Stephenson, Naval Criminal Investigative Service Richard Williams, formerly Director of Defense Security Programs, OSD and additional participants from the Department of State, Joint Chiefs of Staff, and The Tippit Group.
Security Investigations	Gary Maxwell, formerly with the USAF Office of Special Investigations Rodger Raasch, formerly with the Defense Security Service Richard Williams, formerly Director of Defense Security Programs, OSD Thomas W. Woodall, formerly Director of Security, General Services Administration and additional participants from the Defense Security Service and Department of State.
Security Management	Jim Packett, Defense Security Service Jerry Prince, OSD Policy Richard Williams, formerly Director of Defense Security Programs, OSD Thomas W. Woodall, formerly Director of Security, General Services Administration and additional participants from the Defense Threat Reduction Agency, Federal Aviation Agency, and the Defense Security Service Academy.
Communications Security	Eric Cramer, United States Air Force John Frields, formerly with the Office of the Secretary of Defense John Hancock , Department of State Richard Niederkohr, Department of the Army Richard Williams, formerly Director of Defense Security Programs, OSD and additional participants from the Department of State and National Security Agency.
Information Systems Security	Eric Cramer, United States Air Force John Hancock , Department of State Todd Peterson, BAE Systems Holly Ridgeway, Federal Bureau of Investigation Kenneth Quigley, Defense Security Service Richard Williams, formerly Director of Defense Security Programs, OSD and additional participants from the Department of State and Defense Advanced Research Projects Agency.

Exhibit B-3
Agenda for Communications Security Workshop

Agenda

Tuesday, 14 September (day 1) (assemble in Suite 455B. PERSEREC, at 7:45)

Welcome, workshop overview, agenda, and administrative matters (PERSEREC)

Self-introductions (all)

Presentation: Overview of the Joint Security Training Consortium and the National Skill Standards Board methodology (Joe Lualhati)

Presentation: *Baseline Definition of the Security Profession* (John Tippit)

Discussion and Q&A (all)

Working session to validate Communications Security taxonomy (Part 1)
- Overview of session procedures & terminology (Facilitator)
- Review & integrate SME revisions into taxonomy

Wednesday, 15 September (day 2)

Working session to validate Communications Security taxonomy (Part 2)
- Overview of session procedures
- Review & integrate published source documents into taxonomy

Working session to finalize Communications Security taxonomy (Part 3)
- Overview of session procedures
- Review and edit taxonomy

Thursday,16 September (day 3)

Working session to obtain SME ratings of Knowledge and Skill requirements
- Academic and Employability K&S ratings
- Occupational and Technical K&S ratings

Wrap up Review and Discussion (all)
- Review of work accomplished in workshop
- Discussion—comments, critiques, lessons learned

Exhibit B-4
Work Taxonomy Draft 1 for Communications Security Workshop

COMMUNICATIONS SECURITY

Version 1

KEY
I. CWF: Top Level (Critical Work Functions – major responsibilities)
A. KA: Second Level (Key Activities – major duties and tasks)
1. Third Level (Performance Indicators – subtasks)

I. CWF: General Communications Security Activities
A. KA: Assess Organizational Communications Needs
1. Identify who must be communicated with
2. Identify how communications will be accomplished
3. Determine involvement with US National Security Programs
B. KA: Determine Levels of Sensitive Information Involved
1. Determine categories of sensitive information
2. Assess needs to communicate sensitive information
C. KA: Identify Legal and Regulatory Interventions
1. Assess legal and regulatory interventions
2. Identify duties to protect applicable sensitive information
3. Identify communications restrictions
D. KA: Develop Communications Security Plan
1. Define communications architecture
2. Complete a risk assessment
3. Identify safeguards and countermeasures options
4. Develop appropriate policies and procedures
E. KA: Identify Education and Training Needs
1. Identify education and training needs
2. Establish appropriate education and training activities
3. Implement education and training program
II. CWF: Electronic Transmission Security
A. KA: Define System Needs
1. Determine sensitivity of information
2. Identify locations where sensitive information will be located
3. Consider legal issues (Export control, foreign laws, etc)
4. Identify transmission needs between locations
5. Determine the anticipated volume of traffic
6. Consider both the size of initial system(s) and planned/possible growth
B. KA: Identify System Architecture
1. Characterize needs and establish system architecture options
2. Identify supporting system architecture
3. Define equipment needed (equipment listing)
4. Consider appropriate operational standards
C. KA: Obtain, Implement and Manage System
1. Advise on process of obtaining needed equipment and system support
2. Develop the implementation/operations plan
3. Determine education/training needs
4. Establish education/training activities
5. Establish system supervision and audit/reporting processes
III. CWF: Emissions Security
A. KA: Emissions Analysis
1. Conduct emissions vulnerability assessment (Non technical)
2. Determine the need for a technical emission study

3. Identify and document emission vulnerabilities
4. Identify and document emission attenuating features

B. KA: Define Emissions Control Architecture

1. Determine facility control architecture
2. Determine and evaluate safeguard options (Control space, localized emission spike controls, approved equipment, shielded enclosures)
1. Evaluate needs and operational issues
2. Develop the emission control plan
3. Obtain approval from approving authority

C. KA: Implement and Manage Protective Measures

1. Monitor implementation of approved plan
2. Develop appropriate policies and Procedure
3. Establish appropriate education and training activities
4. Establish and implement an appropriate monitoring protocol

IV. CWF: Acoustic Security

A. KA: Identify Locations of Sensitive Discussions/Audio

1. Assess the facility’s layout and identify locations of interest and sound sources
2. Identify the operational patterns of authorized personnel
3. Assess the general presence of unauthorized personnel

B. KA: Assess Acoustic Vulnerabilities

1. Assess the ability of identified locations to retain sound within its perimeter
2. Identify and quantify vulnerabilities
3. Identify the facility’s acoustic risk areas

C. KA: Assess Safeguard/Countermeasures Options

1. Evaluate the facility’s overall physical security and access control program
2. Identify possible physical control measures
3. Identify appropriate acoustical protection measures

D. KA: Develop Acoustic Security Plan

1. Identify applicable regulatory interventions
2. Complete the acoustical risk assessment
3. Develop acoustical security plan to address unacceptable risk
4. Implement and monitor approved plan

V.CWF: COMSEC Materials Security

A. KA: Identify/Establish COMSEC Support Account

1. Identify need/authority for account
2. Request establishment of account
3. Identify COMSEC custodian/alternate and complete indoctrination process
4. Establish duties and responsibilities COMSEC custodian(s)

B. KA: Establish COMSEC Material Control System

1. Identify type and volume of COMSEC materials involved
2. Determine control requirements
3. Identify/establish control policies and procedures
4. Implement material control program

C. KA: Establish Appropriated Safeguards for COMSEC Materials

1. Identify type of COMSEC materials involved
2. Determine safeguarding requirements
3. Assess safeguarding options
4. Identify safeguards and implement

D. KA: Establish COMSEC Materials Handling Procedures

1. Assess the operational use/need of COMSEC materials
2. Develop handling procedures that meet operational and security needs
3. Establish an evaluation protocol to monitor handling procedures and needs

Exhibit B-5
Workshop Terminology

Workshop Term	Commonly Used Term	Definition	Example	Syntax
Critical Work Functions (CWF)	Duties	major responsibilities of work	Oversee facility Physical Security	Action verb + Object
Key Activities (KA)	Tasks	major duties or tasks involved in carrying out a CWF	Address vehicle access controls	Action verb + Object
Performance Indicators (PI)	Subtasks	subtasks required to perform a KA competently	Review facility vehicle access needs	Action verb + Object

Exhibit B-6
List of Concrete Action Verbs

- Acknowledge
- Adjust
- Advise
- Anticipate
- Apply
- Assemble
- Assess
- Assign
- Assist
- Assure
- Attend
- Audit
- Budget
- Build
- Change
- Check
- Clarify
- Coach
- Collaborate
- Collect
- Communicate
- Compile
- Complete
- Comply
- Conduct
- Control
- Counsel
- Create
- Decide
- Define
- Delineate
- Deliver
- Describe
- Design
- Develop
- Direct
- Discuss
- Draft
- Draw
- Edit
- Encourage
- Establish
- Estimate
- Evaluate
- Experiment
- Explain
- Follow
- Forecast
- Formulate
- Gather
- Guide
- Hire
- Identify
- Implement
- Incorporate
- Influence
- Inform
- Initiate
- Inspect
- Inspire
- Install
- Instruct
- Interpret
- Interview
- Inventory
- Invoice
- Keep
- Lead
- Learn
- Leverage
- Locate
- Maintain
- Make
- Manage
- Manufacture
- Measure
- Mediate
- Meet
- Model
- Monitor
- Motivate
- Negotiate
- Network
- Obtain
- Offer
- Operate
- Order
- Participate
- Perform
- Persuade
- Place
- Plan
- Prepare
- Present
- Price
- Prioritize
- Process
- Produce
- Program
- Project
- Promote
- Propose
- Provide
- Publish
- Recommend
- Record
- Repair
- Report
- Research
- Resolve
- Respond
- Review
- Revise
- Schedule
- Select
- Sell
- Serve
- Service
- Set-up
- Share
- Solve
- Summarize
- Support
- Test
- Track
- Train
- Translate
- Update
- Use

Exhibit B-7
Workshop Procedures for Communications Security Workshop

WORKSHOP PROCEDURES:
COMMUNICATIONS SECURITY, 14-16 September 2004

Workshop Configuration

MATERIALS & EQUIPMENT REQUIRED
Handouts (manila folder):
WORKSHOP OVERVIEW (agenda)
Communications Security (taxonomy in outline form)
Workshop Terminology
List of Concrete Action Verbs
Copies of SME revisions to taxonomy based on pre-workshop task (for Task 1)
Copies of published source documents (for Task 2)
Paper & pencils
Computer with *Proxima* projector

TASK 1: Review & Integrate SME Revisions into Taxonomy
(est. time: 2-3 hrs)

Objective:
Review & integrate SME revisions into draft taxonomy
Add, delete, or change *Critical Work Functions*
Add, delete, or change *Key Activities* for *CWFs*
Add, delete, or change *Performance Indicators* for *KAs*

Facilitator:

- Present session OBJECTIVE: To review and & integrate SME revisions into draft taxonomy
- Hand out SME manila folders containing:
  WORKSHOP OVERVIEW (agenda)
  Communications Security (taxonomy in outline form)
  Workshop Terminology
  List of Concrete Action Verbs
- Allow a few minutes for SMEs to prepare comments, if needed

SMEs:

- Each SME recommends his/her changes to group

Facilitator:

- When each SME finishes, poll other participants to determine concurrence/non-concurrence with SME recommendations
- Computer operator:
  - Edit taxonomy to reflect the consensus of each set of SME inputs
  - When all changes have been made, mark revised taxonomy "Version 2"
  - Make hard copies of Version 2 for SMEs

BREAK

TASK 2: Review and Integrate Published Source Documents into Taxonomy
(est. time: 2-3 hrs)

Objective:
Review & integrate source documents into draft taxonomy

Add, delete, or change *Critical Work Functions*
Add, delete, or change *Key Activities* for *CWFs*
Add, delete, or change *Performance Indicators* for *KAs*

Facilitator:

- Present session OBJECTIVE: To review & integrate <u>source documents</u>
- Hand out copies of
  - *COMMUNICATIONS SECURITY* taxonomy (Version 2)

  Source Documents
- Allow individuals or small teams to form based on interests/expertise to work on source documents and materials SMEs have brought to workshop
- Allow teams to prepare comments

SMEs:

- Prepare comments
- Each team presents its recommended changes to group

Facilitator:

- When each team finishes, poll other participants to determine concurrence/non-concurrence with team recommendations
- Computer operator:
  - Edit taxonomy to reflect the consensus of each team's inputs
  - When all changes have been made, mark revised taxonomy "Version 3"
  - Make hard copies of Version 3 for SMEs

BREAK

TASK 3: Conduct Final Review of Taxonomy
(est. time: 2-3 hrs.)

Objectives:
Validate Critical Work functions, Key Activities, and Performance Indicators
Assure that syntax and language conform to NSSB standards

Facilitator:

- Present session OBJECTIVE: To finalize the taxonomy
- Hand out copies of *Communications Security* taxonomy (Version 3)
- Discuss

  Workshop Terminology
  List of Concrete Action Verbs
- Lead discussion through each section of taxonomy

SMEs

- Revise taxonomy based on group consensus
- When finished, submit copies of edited file to computer operator

BREAK

Computer operator (do this off line):

- Edit taxonomy to incorporate changes
- When all changes have been made, mark revised taxonomy "Version 4"
- Make hard copies of Version 4 for SMEs

TASK 4: Obtain K&S Ratings
(est. time: 2 hrs.)

Objectives:
Obtain SME A&E K&S ratings
Obtain SME O&T K&S ratings

Facilitator (J. Lualhati):

- Conduct working session to develop K&S

BREAK

Conclude Workshop
(est. time: 30 minutes)

Moderator:

- Review work accomplished in workshop
- Discuss next steps
- Obtain addresses of SME supervisors for letters of appreciation

END OF WORKSHOP

APPENDIX C

SKILL STANDARDS OVERVIEW FOR USERS OF APPENDICES D-J

SKILL STANDARDS OVERVIEW FOR USERS OF APPENDICES D-J

OVERVIEW AND SUGGESTED READING STRATEGY

This section provides an introduction and overview of the skill standards. It describes the structure, content, and format of the standards with brief excerpts of the information content to illustrate. The complete skill standards are contained separately in Appendices D through J of this report:

Appendix D. Communication Security

Appendix E. Information Security

Appendix F. Information Systems Security

Appendix G. Personnel Security

Appendix H. Physical Security

Appendix I. Security Investigations

Appendix J. Security Management

The appendices are designed for end-users of the standards such as trainers, training evaluators, training designers, job performance evaluators, job designers, and developers of certification programs. This section is duplicated the *Skill Standards Overview* section of the report so that end-users can remove it and appendices D-J and use the combination in stand-alone fashion.

STRUCTURE OF THE STANDARDS

The skill standards fall into two broad categories:

- Work-oriented component—what the worker does to perform the job successfully
- Worker-oriented component—what knowledge and skills (K&S) the worker requires to perform the job successfully

SUBJECT-MATTER EXPERT NOTES

SMEs who helped develop the skill standards sometimes attached explanatory notes to them. The notes, if provided, vary among standards, but addressed issues that the SMEs thought were important but not covered within the standards themselves.

GENERAL PERFORMANCE EXPECTATIONS AND SENIORITY LEVEL

General performance expectations by worker seniority level are summarized in Table C-1.

Table C-1
General Performance Expectations by Worker Seniority Level

Seniority Level		
Entry	**Journeyman**	**Senior**
• Work as a team member • Perform task-level work (associated with key activities) competently • Require major supervision	• Work independently • Perform function- or project-level work at full performance level • Mentor entry-level individuals	• Direct technical work of others • Perform work at the system-level • Serve the role as technical subject-matter expert

WORK-ORIENTED COMPONENT

Definitions

The work-oriented component is described in each set of standards in the form of a three-level taxonomy or outline structured as shown below.

Top Level - Critical Work Functions (CWF1, CWF2, etc.)
Second Level - Key Activities (KA1, KA2, etc.)
Third Level - Performance Indicators (PI)

Table C-2 defines taxonomy terms, gives examples, and illustrates CWF, KA, and PI statement syntax.

Table C-2
Taxonomy Terminology, Examples, and Syntax

Term	Definition	Example	Syntax
Critical Work Function (CWF)	Major responsibilities of work	Define Personnel Security Standards	Action verb + Object
Key Activity (KA)	Major duties or tasks involved in carrying out a CWF	Delineate Employment and Associational Requirements	Action verb + Object
Performance Indicator (PI)	Provides information to judge whether a KA is performed competently	"Employment" security standards are identified, defined, and monitored	Object + Action verb (passive voice)

CWF and KA statements consist of an action verb followed by an object and are written in the *active* voice. PI statements consist of an object followed by an action verb and are written in the *passive* voice. PI statements are concrete actions. KA performance can be judged based on whether or not and how well the underlying PIs are performed.

Example of a Taxonomy

Figure C-1 is an excerpt from the Personnel Security taxonomy. Note that CWF statements are preceded by "CWF" and numbered. KA statements are preceded by "KA" and numbered. PI statements are listed below KA statements without the "PI" label and are unnumbered.

CWF1: Define Personnel Security Standards

- KA1: Delineate Employment and Associational Requirements
    - “Employment” security standards are identified, defined, and monitored
    - Third-party contractor security standards are identified, defined, and monitored
    - Legal and regulatory constraints, if any, are identified, reviewed, and monitored
    - Program plans and/or processing requirements are developed
- KA2: Apply National Security Clearance and/or Specialized Access Requirements
    - Requirements and/or “specialized access” provisions are identified, defined, and monitored
    - Program objectives and processes are identified and developed
    - Legal and regulatory constraints, if any, are identified, reviewed, and monitored
    - Program plans and/or processing requirements are developed
- KA3: Apply Reliability and/or Suitability Concerns
    - High risk task elements requiring greater reliability and/or suitability concerns are identified, defined, and monitored
    - Participation in the determination and evaluation of job sensitivity designations are met
    - Program objectives and processes are identified, defined, and monitored
    - Legal and regulatory constraints, if any, are identified, reviewed, and monitored
    - Program plans and/or processing requirements are developed

Figure C-1 Excerpt of the Personnel Security Taxonomy

Key Activity Knowledge and Performance Level Expectations by Seniority

SMEs estimated the *knowledge* levels required to perform each KA for entry-level, journeyman, and senior security professionals in each discipline using the A-D scale shown in Table C-3.

Table C-3
KA Knowledge Level Scale Definitions

Scale	Description
D-advanced theory	Able to predict, isolate, and resolve problems about the key activity
C-operating principles	Able to identify why and when the key activity must be done and why each step is needed
B-procedures	Able to determine step-by-step procedures for doing the key activity
A-nomenclature	Able to name parts, tools, and simple facts about the key activity

Note that each knowledge level includes all levels below it. For example, a worker with *C-operating principles* proficiency must also possess proficiency at *B-procedures* and *A-nomenclature.*

SMEs also estimated the *performance* levels required on each KA using the 1-4 scale shown in Table C-4.

Table C-4
KA Performance Level Scale Definitions

Scale	Description
4-highly proficient	• Able to complete the KA quickly and accurately • Can tell or show others how to do the KA
3-competent	• Able to do all parts of the KA • Needs only a spot check of completed work
2- partially proficient	• Able to perform most parts of KA • Needs only help on hardest parts
1- extremely limited	• Able to perform simple parts of the KA • Needs to be told or shown how to do most of the KA

Note that each performance level is discrete. Typically, a worker at the *4-highly proficient* level has progressed above *3-competent* and lower levels and performance is no longer accurately described with lower scale levels.

Table C-5 is an excerpt of a table summarizing SME estimates of knowledge and performance levels required on KAs in relation to seniority level for Personnel Security. The left column lists KAs by number, the next three columns to the right show Knowledge level by Seniority, and the three columns on the far right show Performance level by Seniority. Consider the entries to be the minimums required for a worker at each seniority level. Cell entries in the table may be viewed as both text and bar graphs. It is apparent that workers are expected to increase both knowledge and performance level as they gain seniority.

Table C-5
Excerpt of a Table Summarizing Knowledge and Performance Levels Required on KAs in Relation to Seniority Level for Personnel Security

Key Activity	Knowledge Level by Seniority			Performance Level by Seniority		
	Entry	**Journeyman**	**Senior**	Entry	**Journeyman**	**Senior**
1. Delineate Employment and Associational Requirements	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
2. Apply National Security Clearance and/or Specialized Access Requirements	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
3. Apply Reliability and/or Suitability Concerns	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
4. Apply Qualification and Reliability Standards	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high

WORKER-ORIENTED COMPONENT

Definitions

The Worker-Oriented Component consists of three types of K&S: Academic, Employability, and Occupational and Technical. These terms are defined in Table C-6.

Table C-6
Three Types of K&S in Worker-Oriented Component of Skill Standards

Type of K&S	Definition
Academic	K&S associated with the academic disciplines of reading, writing, mathematics and science
Employability	K&S such as teamwork, decision making, and problem solving that apply across a broad ranges of occupations
Occupational and Technical	K&S that apply to the specific type of work

Academic and Employability K&S are combined and called “A&E K&S.” Occupational and Technical K&S are called “OTKS.”

Academic and Employability K&S

There are 23 A&E K&S. Their importance may vary for performance at entry, journeyman, and senior levels. They may also vary in how they affect performance on different CWFs. SMEs reviewed the A&E K&S and judged whether they were *important* or *not applicable* to performance at different seniority levels for each security discipline. SMEs also judged whether or not each A&E K&S was relevant to effective performance on each discipline's CWFs.

Table C-7 shows importance by seniority and relevant CWFs for the first three A&E K&S for Personnel Security. The left column lists and defines each A&E K&S. The next three columns to the right show Importance by Seniority as either important (●) or not applicable (n/a). The eight columns on the far right indicate that the A&E K&S is relevant to the CWF by the presence of a CWF number or not relevant with a blank. (Personnel Security has a total of eight CWFs, but the number varies among disciplines.)

Table C-7
Importance by Seniority and Relevant CWFs for Three A&E K&S for Personnel Security

Academic & Employability Knowledge & Skills	**Importance by Seniority**			**Relevant CWFs**							
	Entry	**Journeyman**	**Senior**	1	2	3	4	5	6	7	8
1. Ability to Learn—Recognize and use learning techniques and recall available information to apply and adapt new knowledge and skills in both familiar and changing situations. Use multiple approaches when learning new things. Assess how one is doing when learning or doing something. Keep up to date technically and know one's own job and related jobs.	●	●	●	1	2	3	4	5	6	7	8
2. Adaptability—Change one's own behavior or work methods to adjust to other people or to changing situations or work demands; be receptive to new information, ideas or strategies to achieve goals.	●	●	●	1	2	3	4	5	6	7	8
3. Analyzing and Solving Problems—Anticipate or identify problems and their causes; develop and analyze potential solutions or improvements using rational and logical processes or innovations and creative approaches when needed.	●	●	●	1	2	3	4	5	6	7	8

Occupational and Technical K&S

Occupational and Technical K&S apply to the specific type of work. Think of them as what the worker must know and be able to do to perform competently. The OTKS apply to workers at all levels of seniority, but OTKS *complexity* increases with seniority. OTKS may also vary in how they affect performance on different CWFs.

SMEs estimated the complexity levels required for each OTKS for entry-level, journeyman, and senior professionals in each security discipline using the 1-5 scale shown in Table C-8.

SMEs also judged whether or not each OTKS is relevant to effective performance on the CWFs for each security discipline.

Table C-9 shows Complexity Level by Seniority and Relevant CWFs for the first three Personnel Security OTKS. The left column lists each OTKS, the next three columns to the right show Complexity Level by Seniority, and the eight columns on the far right indicate that the OTKS is relevant to the CWF by the presence of a CWF number or not relevant with a blank. Complexity Level by Seniority cell entries may be viewed as both text and bar graphs. It is apparent that workers are expected to deal with increasing complexity as they gain seniority. Complexity entries that indicate two levels represent a range. Consider the entries to be the minimums required for a worker at each seniority level.

Table C-8
OTKS Complexity Level Scale Definitions

Scale	Description
5-expert/master K&S required	• Requires ability to independently apply K&S in the most complex, difficult, novel, stressful, or unexpected situations, or situations with high consequences for error • Requires the ability to supervise or lead others in the application of this K&S • Roughly equivalent to the K&S level typically attained through a combination of extensive specialized training or education and an advanced or graduate degree, or at least five years of direct application or use of this knowledge or skill.
4-advanced K&S required	• Requires ability to independently apply K&S in moderately complex, difficult, or stressful situations or situations with moderately high consequences for error • Requires the ability to assist others in the application of this K&S • Roughly equivalent to the K&S level typically attained through extensive specialized training or education or an undergraduate degree or major, or at least two years of direct application or use of this knowledge or skill
3-working or operational K&S required	• Requires ability to independently apply K&S across a range of common applications to meet typical work requirements and having moderate consequences for error • Roughly equivalent to the K&S level typically attained through multiple training courses or a two-year or technical school degree, or 6–24 months of direct application or use of this knowledge or skill
2-basic K&S required	• Application of K&S is limited to relatively routine situations with frequent assistance of others and/or close supervision, and somewhat low consequences of error • Roughly equivalent to the K&S level typically attained through one or two training or academic courses or 1 - 6 months of direct application or use of this knowledge or skill
1-limited K&S required	• General familiarity or awareness of basic concepts or fundamentals, but little or no practical experience • Application of K&S is limited to highly routine, simple, and closely supervised situations with very low consequences of error • Roughly equivalent to the K&S level typically attained through indirect work experience (e.g., observation of others) or less than one month of direct application of this knowledge or skill

Table C-9
Complexity by Seniority and Relevant CWFs for Three Personnel Security OTKS

Occupational & Technical Knowledge & Skills	Complexity Level by Seniority			Relevant to CWFs							
	Entry	Journeyman	Senior								
1. Policies, regulations, guidelines and ethical standards that govern the conduct of Personnel Security Investigations (including, but not limited to): • Investigative standards • Section 1001 and 1905, Title XVIII US Code and other applicable laws • DCID 6/4 • EO 12968 • EO 10450 • Privacy Act 1974 & Freedom of Information Act • Ethical standards (prohibitions and forbidden topics) • Other policies and directives	2-basic 1-limited	3-working	5-expert 4-advanced	1	2	3	4	5	6	7	8
2. Adjudicative guidelines • Allegiance to the United States • Foreign influence • Foreign preference • Sexual Behavior • Personal Conduct • Financial considerations • Alcohol consumption • Drug involvement • Emotional, mental, personality disorders • Criminal conduct • Security violations • Outside activities • Misuse of information technology systems	1-limited	3-working	5-expert	1		3	4	5	6	7	8

3. Investigation concepts, principles, and practices (including, but not limited to): • Types of investigations • Scope of investigations • Coverage requirements for each type of investigation (e.g., Single Scope Background Investigations (SSBI) and SSBI-Periodic Reinvestigations)	1-limited	4-advanced 3-working	5-expert 4-advanced	1		3	4	5	6	7	8

APPENDIX D

SKILL STANDARDS FOR THE COMMUNICATIONS SECURITY DISCIPLINE

SKILL STANDARDS FOR THE COMMUNICATIONS SECURITY DISCIPLINE

OVERVIEW

This appendix contains skill standards for the Communications Security (COMSEC) discipline. It is important to understand skill standards terminology, abbreviations, and what the skill standards are before using this appendix. Appendix C, *Skill Standards Overview for Users of Appendices D-J*, describes the skill standards in detail. Carefully review Appendix C before using this appendix.

The content of this appendix consists of:

- Subject-Matter Expert Notes
- Skill Standard D-1: Communications Security Taxonomy
- Skill Standard D-2: Knowledge and Performance Levels Required on KAs in Relation to Seniority Level for Communications Security
- Skill Standard D-3: A&E K&S Importance by Seniority and Relevant CWFs for Communications Security
- Skill Standard D-4: Complexity Level by Seniority and Relevant CWFs for OTKS for Communications Security

SUBJECT-MATTER EXPERT NOTES

SMEs who contributed to the development of COMSEC skill standards attached two explanatory notes to them. The first concerns the definition of COMSEC. The second concerns the boundaries and possible overlap among COMSEC and related terms. The SME notes are presented verbatim below.

- Note 1. There have been two historical definitions of the term “COMSEC”. The first refers to the security discipline concerned with measures and controls taken to deny unauthorized persons information derived from telecommunications and ensure the authenticity of such telecommunications. Communications security includes cryptosecurity, transmission security, emanations security, and security of COMSEC materials. The second defines COMSEC as the control of encryption equipment and materials. This document treats the latter as a subset of the former.
- Note 2. COMSEC, Information Assurance, Information Security and information processing may or may not be congruent; therefore, requiring appropriate deconfliction. Some organizations such as NSA believe that dealing separately with COMSEC and COMPUSEC issues is not feasible due to the convergence of communications and computing technologies. The “business” of addressing how to provide protection of information against unauthorized disclosure or confidentiality was referred to as Information Systems Security or INFOSEC. Because the term “security” became so closely associated with providing

confidentiality to information, these organizations later adopted the term “Information Assurance” or “IA” to encompass the five security services of Confidentiality, Integrity, Availability, Authenticity, and Non-repudiation.

Skill Standard D-1
Communications Security Taxonomy

CWF1: Develop Communications Security Plan

- KA1: Assess organizational communication needs
  - Communication participants are determined
  - US, foreign, and coalition security program involvements are determined
  - Approaches for accomplishing communications are determined
  - Unique restrictions are determined
- KA2: Determine levels of sensitive information involved
  - Categories of sensitive information are determined
  - Restrictions regarding compartmentation (special considerations) are determined
  - Needs to communicate sensitive information are assessed
- KA3: Identify and address legal, regulatory, and policy requirements
  - Legal, regulatory, and policy requirements are assessed
  - Duties to protect applicable sensitive information are identified
  - Communication restrictions (e.g., legal, export control, foreign laws, Bilateral agreements, etc.) are identified
  - Compliance with all laws, regulations, policies, and industry standards are ensured
- KA4: Identify risks and safeguards
  - Communications architecture is defined
  - Risk assessments are completed
  - Safeguards and countermeasure options are identified
  - Emergency action plans (destruction, contingency, and Continuity of Operations (COOP)) is established
  - Appropriate procedures are developed
- KA5: Identify education and training needs
  - Education and training needs are identified
  - Appropriate education and training activities are established
  - Education and training program is implemented
- KA6: Coordinate with Senior Leadership
  - Recommendations are presented to management
  - Budgetary, legal, technical, and operational constraints related to security are evaluated
  - Decisions are implemented
  - Execution is monitored
  - Evaluative feedback is provided to management as needed

CWF2: Evaluate Electronic Transmission Security

- KA7: Define system needs
  - Sensitivity of information is determined
  - Geographic locations where sensitive information will be transmitted and/or received are identified
  - Anticipated volume of traffic is determined
  - Level and/or type of encryption is determined
  - Both the size of initial system(s) and planned/possible growth are considered
  - Procedures for monitoring and auditing the system are determined
- KA8: Identify systems architectural designs
  - Requirements are interpreted to systems/technology experts
  - Technical experts and users are coordinated to establish security requirements for the architectural solution
  - Recommended solution is submitted to management
- KA9: Obtain, implement, and manage system
  - Advice is provided on process of obtaining needed cryptographic/COMSEC/secure

equipment and system support
    - Security implementation/operations and training plans (including cryptographic network architecture) are developed
    - Plans are applied
    - System supervision and audit/reporting processes are established

CWF3: Establish COMSEC Materials Security

- KA10: Identify/establish COMSEC support account
    - Need and authority are identified
    - Establishment of account is requested
    - Duties and responsibilities associated with the required support are established
    - COMSEC custodian, alternates, or other responsible personnel are identified and trained
- KA11: Establish COMSEC material control system
    - Type and volume of COMSEC materials involved are identified
    - Control requirements are determined
    - Control policies and procedures are identified and established
    - Material control program is implemented
- KA12: Establish appropriate safeguards for COMSEC materials
    - Safeguarding requirements are determined
    - Safeguarding options are assessed
    - Safeguards are identified and implemented
- KA13: Establish COMSEC materials handling procedures
    - Operational use of and need for COMSEC materials are assessed
    - Handling procedures that meet operational and security needs are developed
    - An audit program to monitor and evaluate handling procedures and needs is established
    - COMSEC incident reporting procedures are developed and/or implemented

CWF4: Evaluate Emanations Security

- KA14: Perform emanations analysis
    - Acoustic and electronic emanations vulnerability assessments (nontechnical) are conducted
    - Need for a technical emanation study is determined
    - Emanation vulnerabilities are identified and documented
    - Emanation attenuating features are identified and documented
- KA15: Define emanations control architecture
    - Facility control architecture is determined
    - Safeguard options (controlled and inspectable spaces) are determined and evaluated
    - Needs and operational issues are evaluated
    - A certified TEMPEST Technical Authority is contacted to determine if TEMPEST countermeasures are required
    - Emanations control plan is developed, if required
    - Approval from approving authority is obtained
- KA16: Implement and manage protective measures
    - Implementation of approved plan is monitored
    - Appropriate procedures are developed
    - Appropriate education and training activities are established
    - Appropriate monitoring protocol is established and implemented

Skill Standard D-2
Knowledge and Performance Levels Required on KAs in Relation to Seniority Level for Communications Security

Key Activity	Knowledge Level by Seniority			Performance Level by Seniority		
	Entry	Journeyman	Senior	Entry	Journeyman	Senior
1. Assess organizational communications needs	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
2. Determine levels of sensitive information involved	B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	4-high	4-high
3. Identify and address legal, regulatory, and policy requirements	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
4. Identify risks and safeguards	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
5. Develop education and training	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
6. Coordinate with senior leadership	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
7. Define system needs	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
8. Identify systems architectural designs	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
9. Obtain, implement, and manage system	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
10. Identify/establish COMSEC support account	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
11. Establish COMSEC material control system	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
12. Establish appropriate safeguards for COMSEC materials	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high

Key Activity	Knowledge Level by Seniority			Performance Level by Seniority		
	Entry	Journeyman	Senior	Entry	Journeyman	Senior
13. Establish COMSEC materials handling procedures	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
14. Perform emanations analysis	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
15. Define emanations control architecture	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	2-partial	3-competent	3-competent
16. Implement and manage protective measures	B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	4-high	4-high

Skill Standard D-3
A&E K&S Importance by Seniority and Relevant CWFs
for Communications Security

Academic & Employability Knowledge & Skills	Importance by Seniority			Relevant CWFs			
	Entry	Journeyman	Senior	1	2	3	4
1. Ability to Learn—Recognize and use learning techniques and recall available information to apply and adapt new knowledge and skills in both familiar and changing situations. Use multiple approaches when learning new things. Assess how one is doing when learning or doing something. Keep up to date technically and know one's own job and related jobs.	●	●	●	1	2	3	4
2. Adaptability—Change one's own behavior or work methods to adjust to other people or to changing situations or work demands; be receptive to new information, ideas or strategies to achieve goals.	●	●	●	1	2	3	4
3. Analyzing and Solving Problems—Anticipate or identify problems and their causes; develop and analyze potential solutions or improvements using rational and logical processes or innovations and creative approaches when needed.	●	●	●	1	2	3	4
4. Building Consensus—Build consensus among individuals or groups by facilitating agreements that involve sharing or exchanging resources or resolving difference in such a way as to promote mutual goals and interest; by persuading others to change their points of view or behavior without losing their future support; and by resolving conflicts, confrontation, and disagreements while maintaining productive working relationships.	●	●	●	1	2	3	4
5. Gathering and Analyzing Information—Obtain facts, information or data relevant to a particular problem, question or idea through observation of events or situations, discussions with others, or research or retrieval from written or electronic sources; organize, integrate, analyze and evaluate information.	●	●	●	1	2	3	4
6. Initiative/Motivation—Exert a high level of effort and perseverance towards goal attainment. Work hard to become excellent at doing tasks by setting high standards, paying attention to details, working well and displaying a high level of concentration even when assigned an unpleasant task. Display high standards of attendance, punctuality, enthusiasm, vitality and optimism in approaching and completing tasks. Demonstrate willingness to take on responsibilities and challenges and do what is needed without being asked.	●	●	●	1	2	3	4
7. Integrity/Honesty—Demonstrate dependability, conscientiousness, integrity and accountability. Show commitment to doing the job carefully and correctly. Fulfill obligations and be reliable, responsible and trustworthy. Perform tasks thoroughly and completely. Demonstrate honesty and avoidance of unethical behavior.	●	●	●	1	2	3	4
8. Leading Others—Motivate, inspire, and influence others toward effective individual or teamwork performance, goal attainment, and personal learning and development by serving as a mentor, coach and role model and by providing feedback and recognition or rewards.	n/a	●	●	1	2	3	4
9. Listening—Attend to, receive and correctly interpret verbal communications and directions through cues such as the content and context of the message and the tone, gesture and facial expression of the speaker.	●	●	●	1	2	3	4
10. Maintain Professional Demeanor—Demonstrate credibility and authority in issuing instructions and making requests to individuals and in performing duties. Maintains firm and direct tone of voice, authoritative posture, manner and bearing.	●	●	●	1	2	3	4
11. Making Decisions and Judgments—Make decisions that consider relevant facts and information, potential risks and benefits, and short- and long-term consequences or alternatives.	●	●	●	1	2	3	4

Academic & Employability Knowledge & Skills	Importance by Seniority			Relevant CWFs			
	Entry	Journeyman	Senior	1	2	3	4
12. Mathematics—Understand, interpret and manipulate numeric or symbolic information; solve problems by selecting and applying appropriate quantitative methods such as arithmetic and estimation.	●	●	●	1	2	3	4
13. Organizing and Planning—Organize and structure work for effective performance and goal attainment; set and balance priorities; anticipate obstacles; formulate plans consistent with available human, financial, and physical resources; modify plans or adjust priorities given changing goals or conditions.	●	●	●	1	2	3	4
14. Reading—Understand and use written information that may be presented in a variety of formats, such as text, tables, lists, figures, and diagrams; select reading strategies appropriate to the purpose, such as skimming for highlights, reading for detail, reading for meaning and critical analysis.	●	●	●	1	2	3	4
15. Science—Understand and apply the basic principles of physical, chemical, biological and earth sciences, understand and apply the scientific method, including formulating and stating hypotheses and evaluating them by experimentation or observation.	n/a	n/a	n/a				
16. Self and Career Development—Identify own work and career interests, strengths and limitations; pursue education, training, feedback or other opportunities for learning and development; manage, direct and monitor one's own learning and development.	●	●	●	1	2	3	4
17. Speaking—Express ideas and facts orally in a clear and understandable manner that sustains listener attention and interest; tailor oral communications to the intended purpose and audience.	●	●	●	1	2	3	4
18. Stress Tolerance—Demonstrate maturity, poise and restraint to cope with pressure, stress, criticism, setbacks, personal and work-related problems, etc. Maintain composure, keeping emotions in check, controlling anger, and avoiding aggressive behavior even in very difficult situations. Accept criticism and deal calmly and effectively with high-stress situations.	●	●	●	1	2	3	4
19. Using Information and Communications Technology—Select, access and use necessary information, data, and communications-related technologies, such as basic personal computer applications, telecommunications equipment, Internet, electronic calculators, voice mail, email, facsimile machines and copying equipment to accomplish work activities.	●	●	●	1	2	3	4
20. Using Interpersonal Skills—Interact with others in ways that are friendly, courteous and tactful and that demonstrate respect for individual and cultural differences and for the attitudes and feelings of others.	●	●	●	1	2	3	4
21. Visual Observation—Notice details and take in and recall incoming visual sensory information and use it to make predictions, comparisons and/or evaluations. Recognize differences or similarities, or sensing changes in circumstances or events; discern between relevant visual cues or information and irrelevant or distracting information.	●	●	●	1	2	3	4
22. Working in Teams—Work cooperatively and collaboratively with others to achieve goals by sharing or integrating ideas, knowledge, skills, information, support, resources, responsibility and recognition.	●	●	●	1	2	3	4
23. Writing—Express ideas and information in written form clearly, succinctly, accurately, and in an organized manner; use English language conventions or spelling, punctuation, grammar, and sentence and paragraph structure; and tailor written communication to the intended purpose and audience.	●	●	●	1	2	3	4

Skill Standard D-4
Complexity Level by Seniority and Relevant CWFs for OTKS for Communications Security

Occupational & Technical Knowledge & Skills	Complexity Level by Seniority			Relevant to CWFs			
	Entry	Journeyman	Senior				
1. Concepts, principles, and practices related to protected information loss prevention	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4
2. Developments and advances in communications security systems, methods, equipment, and techniques	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4
3. Methods for analyzing, organizing, compiling, and reporting communications security data	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4
4. Threat, vulnerability, and risk assessment techniques	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4
5. Concepts, practices, and principles associated with recovery/restoration of communications systems	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	
6. Development, preparation, and execution of communications security plans and procedures	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4
7. Development, preparation, and execution of emergency and/or continuity plans	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	
8. Physical security requirements as related to communications security	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4
9. Record management requirements as related to communications security	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4
10. Information System Security/Information Assurance requirements as related to communications security	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4
11. Personnel Security requirements as related to communications security	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4
12. Operations Security Program requirements as related to communications security	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4

Occupational & Technical Knowledge & Skills	Complexity Level by Seniority			Relevant to CWFs			
	Entry	Journeyman	Senior				
13. Information Security requirements as related to communications security	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4
14. Contracting, procurement, acquisition, research, and evaluations related to communications security	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4
15. Design and development of communications security training and instruction	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4
16. Communications security-related funding, manpower requirements, and budgeting programs	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4
17. Development, preparation, and execution of /communications protection program	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4
18. Program evaluation concepts, methods, and techniques	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4
19. Preparation, coordination, and execution of MOU, MOA, Interservice Support Agreements, and Service Level Agreements	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4
20. Protection concepts associated with the information assurance features of availability, integrity, authentication, confidentiality, and non-repudiation	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4
21. Principles, concepts, and methods for information storage, distribution, and transportation	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4
22. Development and advances in emerging technologies (e.g., PDAs, PEDs, wireless networks, internet/intranet, nanotechnology, and artificial intelligence) and their applications and trends in information management	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4
23. Image systems storage (micrographics) including filming, configurations, quality control, hardware, computer output microfilm, film testing, software, and storage	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4
24. Electronic, optical, and other energy transfer of information (e.g., laser) policies and requirements	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4

Occupational & Technical Knowledge & Skills	Complexity Level by Seniority			Relevant to CWFs			
	Entry	Journeyman	Senior				
25. Classification management and other protected information concepts and terms (including concepts and principles of original and derivative classification)	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4
26. Security fault analysis	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4
27. Development, preparation, and execution of communications security presentations and briefings	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4
28. Threat situation and their impact (including, but not limited to counter-intelligence and counter-terrorism, and personal safety and environment)	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4
29. Concepts, principles, and practices associated with standard reporting formats	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	
30. Special category programs as they apply to Communications Security	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	
31. Foreign threat (e.g., countries & organizations)	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4
32. Interviewing techniques	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4
33. Concepts, principles, and practices of proper control of records	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4
34. Risk management concepts, principles, and practices	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4
35. Laws and regulations governing the release of information (e.g., Freedom of Information Act (FOIA), Privacy Act)	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4
36. Security analysis methods and techniques (including, but not limited to methods for analyzing security incident trends and statistical data)	1-limited	4-advanced 3-working	5-expert 4-advanced	1	2	3	4
37. Regulations and procedures related to controlled cryptographic gear and items	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4

Occupational & Technical Knowledge & Skills	Complexity Level by Seniority			Relevant to CWFs			
	Entry	Journeyman	Senior				
38. Encryption concept, principles, methodologies, and techniques	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	
39. Cryptographic key management concepts, principles, methodologies, and techniques	2-basic	4-advanced 3-working	5-expert 4-advanced			3	
40. COMSEC inspection and auditing concepts, principles, methodologies, and techniques	2-basic	4-advanced 3-working	5-expert 4-advanced			3	
41. COMSEC material classification, disposition, and retention	2-basic	4-advanced 3-working	5-expert 4-advanced			3	
42. Courier service	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	
43. Secure telecommunications basic, concepts, and principles	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4
44. Access requirements to classified and unclassified COMSEC materials	2-basic	4-advanced 3-working	5-expert 4-advanced			3	
45. COMSEC account concepts, principles, and methodologies (including requirements; account upgrades, downgrades, and conversions; selection of COMSEC custodian and alternate)	2-basic	4-advanced 3-working	5-expert 4-advanced			3	
46. Procedures for handling keying material	2-basic	4-advanced 3-working	5-expert 4-advanced			3	
47. Secure Voice/Data guidelines and requirements (e.g., STU-III, STE, VOIP STE, etc.)	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	
48. Incident reporting requirements and evaluation guidelines	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4
49. COMSEC incident reporting	2-basic	4-advanced 3-working	5-expert 4-advanced			3	
50. Concepts, principles, and practices related to protected information loss prevention	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4

Occupational & Technical Knowledge & Skills	Complexity Level by Seniority			Relevant to CWFs			
	Entry	Journeyman	Senior				
51. Developments and advances in communications security systems, methods, equipment, and techniques	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4
52. Methods for analyzing, organizing, compiling, and reporting communications security data	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4
53. Threat, vulnerability, and risk assessment techniques	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4
54. Concepts, practices, and principles associated with recovery/restoration of communications systems	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	
55. Development, preparation, and execution of communications security plans and procedures	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4
56. Development, preparation, and execution of emergency and/or continuity plans	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	
57. Physical security requirements as related to communications security	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4
58. Record management requirements as related to communications security	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4
59. Information System Security/Information Assurance requirements as related to communications security	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4
60. Personnel Security requirements as related to communications security	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4
61. Operations Security Program requirements as related to communications security	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4
62. Information Security requirements as related to communications security	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4
63. Contracting, procurement, acquisition, research, and evaluations related to communications security	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4

Occupational & Technical Knowledge & Skills	Complexity Level by Seniority			Relevant to CWFs			
	Entry	Journeyman	Senior				
64. Design and development of communications security training and instruction	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4
65. Communications security-related funding, manpower requirements, and budgeting programs	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4
66. Development, preparation, and execution of communications protection program	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4
67. Program evaluation concepts, methods, and techniques	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4
68. Preparation, coordination, and execution of MOU, MOA, Interservice Support Agreements, and Service Level Agreements	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4
69. Protection concepts associated with the information assurance features of availability, integrity, authentication, confidentiality, and non-repudiation	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4
70. Principles, concepts, and methods for information storage, distribution, and transportation	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4
71. Development and advances in emerging technologies (e.g., PDAs, PEDs, wireless networks, internet/intranet, nanotechnology, and artificial intelligence) and their applications and trends in information management	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4
72. Image systems storage (micrographics) including filming, configurations, quality control, hardware, computer output microfilm, film testing, software, and storage	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4
73. Electronic, optical, and other energy transfer of information (e.g., laser) policies and requirements	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4
74. Classification management and other protected information concepts and terms (including concepts and principles of original and derivative classification)	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4
75. Security fault analysis	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4

Occupational & Technical Knowledge & Skills	Complexity Level by Seniority			Relevant to CWFs			
	Entry	Journeyman	Senior				
76. Development, preparation, and execution of communications security presentations and briefings	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4
77. Threat situation and their impact (including, but not limited to counter-intelligence and counter-terrorism, and personal safety and environment)	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4
78. Concepts, principles, and practices associated with standard reporting formats	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	
79. Special category programs as they apply to Communications Security	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	
80. Foreign threat (e.g., countries & organizations)	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4
81. Interviewing techniques	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4
82. Concepts, principles, and practices of proper control of records	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4
83. Risk management concepts, principles, and practices	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4
84. Laws and regulations governing the release of information (e.g., Freedom of Information Act (FOIA), Privacy Act)	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4
85. Security analysis methods and techniques (including, but not limited to methods for analyzing security incident trends and statistical data)	1-limited	4-advanced 3-working	5-expert 4-advanced	1	2	3	4
86. Regulations and procedures related to controlled cryptographic gear and items	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4
87. Encryption concept, principles, methodologies, and techniques	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	
88. Cryptographic key management concepts, principles, methodologies, and techniques	2-basic	4-advanced 3-working	5-expert 4-advanced			3	

Occupational & Technical Knowledge & Skills	Complexity Level by Seniority			Relevant to CWFs			
	Entry	Journeyman	Senior				
89. COMSEC inspection and auditing concepts, principles, methodologies, and techniques	2-basic	4-advanced 3-working	5-expert 4-advanced			3	
90. COMSEC material classification, disposition, and retention	2-basic	4-advanced 3-working	5-expert 4-advanced			3	
91. Courier service	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	
92. Secure telecommunications basic, concepts, and principles	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4
93. Access requirements to classified and unclassified COMSEC materials	2-basic	4-advanced 3-working	5-expert 4-advanced			3	
94. COMSEC account concepts, principles, and methodologies (including requirements; account upgrades, downgrades, and conversions; selection of COMSEC custodian and alternate)	2-basic	4-advanced 3-working	5-expert 4-advanced			3	
95. Procedures for handling keying material	2-basic	4-advanced 3-working	5-expert 4-advanced			3	
96. Secure Voice/Data guidelines and requirements (e.g., STU-III, STE, VOIP STE, etc.)	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	
97. Incident reporting requirements and evaluation guidelines	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4
98. COMSEC incident reporting	2-basic	4-advanced 3-working	5-expert 4-advanced			3	

APPENDIX E

SKILL STANDARDS FOR THE INFORMATION SECURITY DISCIPLINE

SKILL STANDARDS FOR THE INFORMATION SECURITY DISCIPLINE

OVERVIEW

This appendix contains skill standards for the Information Security (INFOSEC) discipline. It is important to understand skill standards terminology, abbreviations, and what the skill standards are before using this appendix. Appendix C, *Skill Standards Overview for Users of Appendices D-J*, describes the skill standards in detail. Carefully review Appendix C before using this appendix.

The content of this appendix consists of:

- Subject-Matter Expert Notes
- Skill Standard E-1: Information Security Taxonomy
- Skill Standard E-2: Knowledge and Performance Levels Required on KAs in Relation to Seniority Level for Information Security
- Skill Standard E-3: A&E K&S Importance by Seniority and Relevant CWFs for Information Security
- Skill Standard E-4: Complexity Level by Seniority and Relevant CWFs for OTKS for Information Security

SUBJECT-MATTER EXPERT NOTES

SMEs who contributed to the development of INFOSEC skill standards attached two explanatory notes to them. The first concerns the computer and ancillary skills of INFOSEC professionals. The second concerns the need to coordinate with information systems security professionals. The SME notes are presented verbatim below.

- Note 1. In addition to having entry level computer skills, information security professionals must have a fundamental understanding of the protection concepts associated with information assurance (i.e., availability, integrity, authentication, confidentiality, and non-repudiation). These are necessary to protect data in information systems and networks.
- Note 2. It is understood throughout this document that required coordination must be accomplished with information systems security professionals in all instances wherein protected data is placed into automated systems and others as necessary (e.g., first responders, safety and environmental officials).

Skill Standard E-1
Information Security Taxonomy

CWF1: Identify Protected Information

- KA1: Evaluate Information Assets
    - The organization’s mission and/or operational objectives are reviewed to assess information protection requirements
    - Critical information needs and/or sensitivities are determined
    - Applicable legal and regulatory requirements and prohibitions are identified
    - Information profile for organization and/or entity is developed
    - Individuals with authority to identify protected information are identified
- KA2: Identify Information Requiring Protection
    - Identifier for each category of protected information is established or determined
    - Appropriate notification and/or warning notices are developed or determined
    - Inconsistencies within the categories of protected information are identified
    - Appropriate corrective actions regarding inconsistencies are determined
    - Classified and unclassified controlled National Security Information and atomic energy information is identified
    - Trade secret and/or proprietary information is identified
    - Third party information held under a duty to protect is identified
    - Compartmented information (e.g., SAPs/SARs, intelligence and weapons of mass destruction) or critical infrastructure information is identified
    - Foreign government information and/or specialized treaty information is identified
    - Information essential to the accomplishment of organizational missions and retention of historical records is identified
    - Other intellectual property that requires protection is identified
    - Other information whose protection is required by law, regulation, or agency policy is identified
    - Sensitivity resulting from data aggregation is identified
- KA3: Re-evaluate Program Processes
    - Mandatory and/or desired periodic review schedules are identified
    - Review processes and/or authorities are determined and/or established
    - Implementing policies and procedures are developed
    - Documentation and notification needs are determined
    - Key indicators that would initiate evaluation outside periodic reviews are identified
- KA4: Obtain or Produce Guidance for Identifying Protected Information
    - The authority requiring protection for each category of information is identified
    - Guidance for identifying all categories of protected information is obtained and/or produced
    - Protected information guidance is continuously monitored for changes and updates
    - Operational personnel are made aware of changes and updates to protected information guidance
    - Use of protected information guidance by operational personnel is continuously monitored to ensure that latest version is applied

CWF2: Define the Information Protection Program

- KA5: Identify Requirements for Authorized Access
    - Legal and regulatory requirements for mandatory restrictions are reviewed
    - Any additional conditions of access to include restrictions on compartmented and other categories of information are determined
    - Disclosure strategies are determined
    - Results are documented
- KA6: Establish Responsibility and Duty to Protect
    - Acceptable methods of establishing the responsibility and duty to protect are identified
    - Verification protocols for imposed duties to protect are developed
    - Special safeguarding measures needed to protect information are determined and, if necessary, measures are coordinated with the appropriate security specialists and other

    - disciplines (e.g., environmental and safety personnel)
    - Strategy for establishing duty to protect is developed
    - Non-disclosure agreements are identified and developed, where appropriate
- KA7: Apply Need-to-Know Principle
    - Need-to-know standards are adopted to address what will be shared and/or restricted by category of “broad access” (e.g., SIPRNET)
    - Methods for applying need-to-know standards to the information selected for protection are identified
    - Need-to-know application and/or process methods are defined
    - Need-to-know granting authorities are identified
    - Need-to-know implementation policy and procedures are developed
- KA8: Establish Information Production Procedures
    - Assets that can be used to generate protected information including specific areas, specific equipment, and required controls are identified
    - Positions that authorize production of protected information (original and derivative) are identified
    - Required emission and emanation controls are identified
- KA9: Control Protected Information Received and Generated
    - Control requirements for receipts and companion documentation, where defined, are identified
    - Control locations of receipt and generation are determined
    - Documentation needed for receipt and/or generation is identified
    - Documentation procedures are defined
- KA10: Control Dissemination of Protected Information
    - Information requiring dissemination documentation is identified
    - Legal and regulatory requirements are reviewed
    - Methods of dissemination documentation are identified/assessed/selected
    - Records management requirements (e.g., records of permanent historical value) are identified
    - Policy and procedures for documenting the dissemination are developed
- KA11: Establish Visitor Control Procedures (Access to information)
    - Visitor authorization authorities are identified
    - Visitor exclusion areas are identified
    - Visitor escort procedures are developed

CWF3: Administer Handling Procedures

- KA12: Determine Markings and/or Warnings
    - Laws and regulations for marking and warning standards and requirements are reviewed
    - Categories of protected information to include specialized restrictions applicable to compartmented, diplomatic, foreign, and treaty information are determined
    - Mediums that will contain protected information are evaluated and determined
    - Marking and/or warning procedures for each medium are developed
    - Procedures to ensure that all protected information material is properly identified and marked are established
- KA13: Ensure Accountability
    - Laws, agreements, and regulations are reviewed for standards and requirements
    - Accountability requirements for media containing protected information are determined
    - Media that contain information requiring accountability are identified
    - Appropriate accountability procedures are developed
- KA14: Ensure Protection While In Use
    - Laws and regulations are reviewed for standards and requirements
    - Specifics about how protected information will be used to meet operational needs are determined
    - Locations and types of uses are determined
    - Policy and/or procedures to meet operational and protective standards needs are developed

  - Special “in use” restrictions for selected data such as Presidential correspondence are identified and monitored
  - Information required to perform assigned tasks and functions is identified
  - Information no longer needed to perform assigned tasks and functions are identified
- KA15: Assess Storage Requirements
  - Laws and regulations are reviewed for standards and requirements
  - Physical and digital storage needs are assessed
  - Storage options that meet operational and/or security needs are identified
  - Policy and/or procedures to meet operational and/or security needs are developed
  - Specialized requirements are coordinated with others, as needed
- KA16: Establish Transmission and Transportation Controls
  - Laws and regulations are reviewed for standards and requirements
  - Needs for operational transmission and transportation are assessed
  - Acceptable transmission and transportation methods and options are identified
  - Secure transmission and transportation capabilities for sending and receiving materials are identified
  - Transmission and transportation plan is developed to meet operational and/or security needs to include two-person rules or other restrictions, if required
- KA17: Establish Disposition and/or Destruction Procedures
  - Laws and regulations are reviewed for standards and requirements
  - Operational disposition and/or destruction needs are assessed
  - Appropriate disposition and/or destruction methods and options are identified
  - Policy and/or procedures to meet operational and/or security needs are developed
  - Compliance with program disposition and/or destruction requirements are ensured
  - Contingency plans for emergency disposition and/or destruction procedures to include media containing protected information and classified equipment are developed
- KA18: Manage the Changing or Ending of Protection
  - Laws and regulations are reviewed for standards and requirements
  - Events and/or conditions that justify and/or require the changing or ending of protection are determined
  - Appropriate processes and methods for changing and/or ending protection are established
  - Policy and/or procedures to meet operational and/or security needs are developed
  - Compliance requirements for records management are identified

CWF4: Evaluate Program Effectiveness

- KA19: Evaluate Program Processes
  - Qualitative and quantitative indicators to detect process problems and/or failures are identified, and methods to sample
  - indicators are developed
  - Process for internal and/or external evaluations and assessments (e.g., audits and reviews) is implemented
  - Administrative inquiry of instances of loss, compromise, or suspected compromise is conducted
  - Results are analyzed to identify issues
  - Results are documented and disseminated, as appropriate
  - Necessary corrective actions are identified
  - Appropriate reports to promulgate results of evaluation are prepared
- KA20: Conduct Failure Analysis
  - Reports of incidents and/or system failures are received and reviewed
  - Analysis to determine failure elements are conducted
  - Consequence and/or potential consequence of failure is established
  - Damage assessments are initiated
  - Results are documented and disseminated, as appropriate
  - Appropriate corrective actions are recommended
  - Appropriate reporting of incidents, as required by regulation, is ensured
- KA21: Conduct Trend Analysis

  - Evaluation and/or failure analysis reports are obtained
  - Reports are reviewed to identify trend issues
  - Availability of data for information security reporting requirements (e.g., Information Security Oversight Office) is ensured
  - Corrective actions and/or policy changes are identified and/or recommended

CWF5: Perform Other Information Security Activities

- KA22: Establish Export, Munitions, and Other Controls
  - Legal and/or regulatory requirements are reviewed to determine applicability of export controls, munitions, and other
  - restrictions
  - Organization's products and/or technology inventory are reviewed
  - Exposure profile for foreign nationals and/or representatives of foreign interests are reviewed
  - Procedures to comply with requirements are developed
- KA23: Develop Treaty Inspection Control
  - Legal and regulatory requirements are reviewed to determine applicability
  - Organization's products and/or technology inventory are reviewed
  - Disclosure criteria (e.g., exposure profiles) and locations of sensitive information to include compartmented and other specialized information are reviewed
  - Access requirements are reviewed and compared to facility design
  - Procedures to protect information and comply with treaty obligations are developed
- KA24: Develop Research, Technology, Evaluation, and Acquisition Controls
  - Legal and regulatory requirements are reviewed to determine applicability
  - Organization's research, technology, evaluation, and acquisition activities are reviewed
  - Procedures to comply with requirements to include industrial security are developed

CWF6: Manage Program Implementation

- KA25: Develop Policies and Procedures
  - Appropriate media for promulgation of policy and procedural requirements are determined
  - Guidance are prepared and disseminated
  - Advice and assistance in implementing requirements are provided in elements of the organization
- KA26: Assist in Program Implementation
  - Technical advice and assistance in performance of security functions (e.g., the development and
  - maintenance of protected information guidance) are provided
  - Responses to program-related questions from operational personnel are provided
  - Assistance in developing alternative procedures in special situations is provided
  - Requests for waivers of and exceptions to requirements are analyzed
  - Recommendations or decisions on requests for waivers of and exceptions to requirements are made
  - Changes in missions, functions, organizations, and information sensitivity that could affect security programs are continuously monitored and necessary changes to procedures are devised
- KA27: Conduct Outreach Activities
  - Independent judgment and discretion is exercised in order to effectively represent the organization's positions to external officials
  - Materials for briefings, meetings, or conferences are developed and presentations conducted as necessary
  - Liaison activities are conducted with governmental personnel (inside and outside the organization), representatives of industry and other agencies, security professional associations, and the public

CWF7: Establish Security Education, Training, and Awareness Programs

- KA28: Perform Needs Assessment
  - Legal and regulatory requirements for information security education are determined

  - General security education needs for the total organization population and separate population segments are determined
  - Security education needs of special categories of personnel (e.g., original classifiers, declassifiers, people handling protected information) are determined
- KA29: Develop and Execute Programs
  - Security education briefings, classes, and other presentations are prepared and presented as required
  - Access to education and training activities conducted by others, including distance learning, are
  - facilitated
  - Utility of training alternatives (e.g., job aids, ready reference materials) is determined
  - Training alternatives (e.g., job aids, ready reference materials) are obtained or created
  - General and specialized threat and vulnerability awareness presentations are prepared and delivered
  - Awareness aids (e.g., posters, computer media) are obtained or created and disseminated
  - Appropriate descriptions of organization’s programs, policies, or procedures are given to appropriate personnel

Skill Standard E-2
Knowledge and Performance Levels Required on KAs in Relation to Seniority Level for Information Security

Key Activity	Knowledge Level by Seniority			Performance Level by Seniority		
	Entry	Journeyman	Senior	Entry	Journeyman	Senior
1. Evaluate Information Assets	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
2. Identify Information Requiring Protection	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
3. Re-evaluate Program Processes	A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	1-limited	3-competent	4-high
4. Obtain or Produce Guidance for Identifying Protected Information	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
5. Identify Requirements for Authorized Access	B-procedures A-nomenclature	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
6. Establish Responsibility and Duty to Protect	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
7. Apply Need-to-Know Principle	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
8. Establish Information Production Procedures	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
9. Control Protected Information Received and Generated	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
10. Control Dissemination of Protected Information	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
11. Establish Visitor Control Procedures (Access to Information)	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
12. Determine Markings and/or Warnings	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high

Key Activity	Knowledge Level by Seniority			Performance Level by Seniority		
	Entry	Journeyman	Senior	Entry	Journeyman	Senior
13. Ensure Accountability	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
14. Ensure Protection While in Use	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
15. Assess Storage Requirements	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
16. Establish Transmission and Transportation Controls	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
17. Establish Disposition and/or Destruction Procedures	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
18. Manage the Changing or Ending of Protection	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
19. Evaluate Program Processes	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
20. Conduct Failure Analysis	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
21. Conduct Trend Analysis	A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	1-limited	3-competent	4-high
22. Establish Export, Munitions, and Other Controls	A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	1-limited	3-competent	4-high
23. Develop Treaty Inspection Control	A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	1-limited	3-competent	4-high
24. Develop Research, Technology, Evaluation, and Acquisition Control	A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	1-limited	3-competent	4-high
25. Develop Policies and Procedures	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high

Key Activity	Knowledge Level by Seniority			Performance Level by Seniority		
	Entry	Journeyman	Senior	Entry	Journeyman	Senior
26. Assist in Program Implementation	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
27. Conduct Outreach Activities	A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	1-limited	3-competent	4-high
28. Perform Needs Assessment	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
29. Develop and Execute Program	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high

Skill Standard E-3
A&E K&S Importance by Seniority and Relevant CWFs for Information Security

Academic & Employability Knowledge & Skills	Importance by Seniority			Relevant CWFs						
	Entry	Journeyman	Senior	1	2	3	4	5	6	7
1. Ability to Learn—Recognize and use learning techniques and recall available information to apply and adapt new knowledge and skills in both familiar and changing situations. Use multiple approaches when learning new things. Assess how one is doing when learning or doing something. Keep up to date technically and know one's own job and related jobs.	●	●	●	1	2	3	4	5	6	7
2. Adaptability—Change one's own behavior or work methods to adjust to other people or to changing situations or work demands; be receptive to new information, ideas or strategies to achieve goals.	●	●	●	1	2	3	4	5	6	7
3. Analyzing and Solving Problems—Anticipate or identify problems and their causes; develop and analyze potential solutions or improvements using rational and logical processes or innovations and creative approaches when needed.	●	●	●	1	2	3	4	5	6	7
4. Building Consensus—Build consensus among individuals or groups by facilitating agreements that involve sharing or exchanging resources or resolving difference in such a way as to promote mutual goals and interest; by persuading others to change their points of view or behavior without losing their future support; and by resolving conflicts, confrontation, and disagreements while maintaining productive working relationships.	●	●	●	1	2	3	4	5	6	7
5. Gathering and Analyzing Information—Obtain facts, information or data relevant to a particular problem, question or idea through observation of events or situations, discussions with others, or research or retrieval from written or electronic sources; organize, integrate, analyze and evaluate information.	●	●	●	1	2	3	4	5	6	7
6. Initiative/Motivation—Exert a high level of effort and perseverance towards goal attainment. Work hard to become excellent at doing tasks by setting high standards, paying attention to details, working well and displaying a high level of concentration even when assigned an unpleasant task. Display high standards of attendance, punctuality, enthusiasm, vitality and optimism in approaching and completing tasks. Demonstrate willingness to take on responsibilities and challenges and do what is needed without being asked.	●	●	●	1	2	3	4	5	6	7
7. Integrity/Honesty—Demonstrate dependability, conscientiousness, integrity and accountability. Show commitment to doing the job carefully and correctly. Fulfill obligations and be reliable, responsible and trustworthy. Perform tasks thoroughly and completely. Demonstrate honesty and avoidance of unethical behavior.	●	●	●	1	2	3	4	5	6	7
8. Leading Others—Motivate, inspire, and influence others toward effective individual or teamwork performance, goal attainment, and personal learning and development by serving as a mentor, coach and role model and by providing feedback and recognition or rewards.	n/a	●	●	1	2	3	4	5	6	7

Academic & Employability Knowledge & Skills	Importance by Seniority			Relevant CWFs						
	Entry	Journeyman	Senior	1	2	3	4	5	6	7
9. Listening—Attend to, receive and correctly interpret verbal communications and directions through cues such as the content and context of the message and the tone, gesture and facial expression of the speaker.	●	●	●	1	2	3	4	5	6	7
10. Maintain Professional Demeanor—Demonstrate credibility and authority in issuing instructions and making requests to individuals and in performing duties. Maintains firm and direct tone of voice, authoritative posture, manner and bearing.	●	●	●	1	2	3	4	5	6	7
11. Making Decisions and Judgments—Make decisions that consider relevant facts and information, potential risks and benefits, and short- and long-term consequences or alternatives.	●	●	●	1	2	3	4	5	6	7
12. Mathematics—Understand, interpret and manipulate numeric or symbolic information; solve problems by selecting and applying appropriate quantitative methods such as arithmetic and estimation.	n/a	●	●	1	2	3	4	5	6	7
13. Organizing and Planning—Organize and structure work for effective performance and goal attainment; set and balance priorities; anticipate obstacles; formulate plans consistent with available human, financial, and physical resources; modify plans or adjust priorities given changing goals or conditions.	●	●	●	1	2	3	4	5	6	7
14. Reading—Understand and use written information that may be presented in a variety of formats, such as text, tables, lists, figures, and diagrams; select reading strategies appropriate to the purpose, such as skimming for highlights, reading for detail, reading for meaning and critical analysis.	●	●	●	1	2	3	4	5	6	7
15. Science—Understand and apply the basic principles of physical, chemical, biological and earth sciences, understand and apply the scientific method, including formulating and stating hypotheses and evaluating them by experimentation or observation.	n/a	n/a	n/a							
16. Self and Career Development—Identify own work and career interests, strengths and limitations; pursue education, training, feedback or other opportunities for learning and development; manage, direct and monitor one's own learning and development.	●	●	●	1	2	3	4	5	6	7
17. Speaking—Express ideas and facts orally in a clear and understandable manner that sustains listener attention and interest; tailor oral communications to the intended purpose and audience.	●	●	●	1	2	3	4	5	6	7
18. Stress Tolerance—Demonstrate maturity, poise and restraint to cope with pressure, stress, criticism, setbacks, personal and work-related problems, etc. Maintain composure, keeping emotions in check, controlling anger, and avoiding aggressive behavior even in very difficult situations. Accept criticism and deal calmly and effectively with high-stress situations.	●	●	●	1	2	3	4	5	6	7

Academic & Employability Knowledge & Skills	Importance by Seniority			Relevant CWFs						
	Entry	Journeyman	Senior	1	2	3	4	5	6	7
19. Using Information and Communications Technology—Select, access and use necessary information, data, and communications-related technologies, such as basic personal computer applications, telecommunications equipment, Internet, electronic calculators, voice mail, email, facsimile machines and copying equipment to accomplish work activities.	●	●	●	1	2	3	4	5	6	7
20. Using Interpersonal Skills—Interact with others in ways that are friendly, courteous and tactful and that demonstrate respect for individual and cultural differences and for the attitudes and feelings of others.	●	●	●	1	2	3	4	5	6	7
21. Visual Observation—Notice details and take in and recall incoming visual sensory information and use it to make predictions, comparisons and/or evaluations. Recognize differences or similarities, or sensing changes in circumstances or events; discern between relevant visual cues or information and irrelevant or distracting information.	●	●	●	1	2	3	4	5	6	7
22. Working in Teams—Work cooperatively and collaboratively with others to achieve goals by sharing or integrating ideas, knowledge, skills, information, support, resources, responsibility and recognition.	●	●	●	1	2	3	4	5	6	7
23. Writing—Express ideas and information in written form clearly, succinctly, accurately, and in an organized manner; use English language conventions or spelling, punctuation, grammar, and sentence and paragraph structure; and tailor written communication to the intended purpose and audience.	●	●	●	1	2	3	4	5	6	7

Skill Standard E-4
Complexity Level by Seniority and Relevant CWFs for OTKS for Information Security

Occupational & Technical Knowledge & Skills	Complexity Level by Seniority			Relevant to CWFs						
	Entry	Journeyman	Senior							
1. Information security regulations and processes including classification status determination, assessment procedures, security, classification, declassification, reclassification, marking, control, accountability, and safeguarding of records	2-basic	4-advanced	5-expert	1	2	3	4	5	6	7
2. Developments and advances in information security systems, methods, equipment, and techniques	2-basic	4-advanced 3-working	5-expert 4-advanced			3		5	6	7
3. Methods for analyzing, organizing, compiling, and reporting information security data	2-basic 1-limited	4-advanced 3-working	5-expert	1	2	3	4	5	6	
4. Threat, vulnerability, and risk assessment techniques associated with information security	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4		6	
5. Concepts, practices, and principles associated with recovery/restoration of information security program data	2-basic 1-limited	4-advanced 3-working	5-expert 4-advanced		2	3	4		6	7
6. Development, preparation, and execution of information security plans	2-basic 1-limited	4-advanced 3-working	5-expert 4-advanced	1	2	3	4		6	
7. Development, preparation, and execution of information security policies and procedures	2-basic 1-limited	4-advanced	5-expert			3	4		6	
8. Concepts, principles, and practices related to protected information loss prevention as it relates to information security	2-basic 1-limited	4-advanced	5-expert 4-advanced	1	2	3	4		6	7
9. Development, preparation, and execution of emergency and/or continuity plans as it related to information security	2-basic 1-limited	4-advanced 3-working	5-expert 4-advanced	1	2	3	4		6	7

Occupational & Technical Knowledge & Skills	Complexity Level by Seniority			Relevant to CWFs						
	Entry	Journeyman	Senior							
10. Laws and regulations governing the release of information (e.g., FOIA, Privacy Act), and Statutes and Executive Orders governing the protection of specific types of records (e.g., EO 12958 as amended, Atomic Energy Act, Section 119, Title X, U.S. Code). This includes (but is not limited to): (1) regulations, concepts, and principles related to data aggregation; (2) security assistance policies including laws, regulations, and policies controlling U.S. transfer of arms and services to foreign governments and international organizations (e.g., Arms Export Control Act of 1976).	2-basic	4-advanced	5-expert		2	3		5	6	
11. Physical security requirements as related to information security	2-basic	4-advanced	5-expert		2	3			6	
12. Record management requirements as related to information security	2-basic 1-limited	4-advanced 3-working	5-expert 4-advanced		2	3				
13. Information System Security requirements as related to information security	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3			6	7
14. Personnel Security Program requirements as related to information security	2-basic 1-limited	4-advanced 3-working	5-expert 4-advanced	1	2	3			6	7
15. Operations Security Program requirements as related to information security	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4	5	6	7
16. Contracting, procurement, acquisition, research, and technical proposal evaluations related to information security (including content and format of technical contract specifications)	2-basic 1-limited	4-advanced 3-working	5-expert 4-advanced	1	2	3		5	6	
17. Design and development of information security training and instruction	2-basic 1-limited	4-advanced	5-expert 4-advanced				4		6	7
18. Information security-related funding, manpower requirements, and budgeting programs	2-basic 1-limited	4-advanced 3-working	5-expert 4-advanced	1	2	3	4			7

Occupational & Technical Knowledge & Skills	Complexity Level by Seniority			Relevant to CWFs						
	Entry	Journeyman	Senior							
19: Communications Security Program requirements as related to information security	2-basic	4-advanced	5-expert		2	3	4	5	6	7
20: Information security regulations and processes including protected information status, determination, assessment procedures, security, marking, control, accountability, and safeguarding of records	2-basic	4-advanced	5-expert	1	2	3		5	6	
21. Development, preparation, and execution of information protection program (including the development, preparation, and application of protected information guidelines)	2-basic 1-limited	4-advanced 3-working	5-expert	1	2	3	4	5	6	
22. Development, preparation, and execution of protected information handling procedures	2-basic	4-advanced	5-expert	1	2	3			6	7
23. Program evaluation concepts, methods, and techniques	2-basic	4-advanced	5-expert				4			
24. Preparation, coordination, and execution of MOU, MOA, Interservice Support Agreements, and Service Level Agreements	2-basic 1-limited	4-advanced 3-working	5-expert 4-advanced	1	2	3		5	6	
25. Protection concepts associated with the information assurance features of availability, integrity, authentication, confidentiality, and non-repudiation	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4		6	
26. Integration of information technologies (e.g., biometrics, information tracking, bar code, geo-spatial information)	2-basic 1-limited	4-advanced 3-working	5-expert 4-advanced	1	2	3			6	
27. Principles, concepts, and methods for information storage, distribution, and transportation	2-basic	4-advanced	5-expert		2	3			6	
28. Developments and advances in emerging technologies (e.g., PDAs, PEDs, wireless networks, internet/intranet, nanotechnology, and artificial intelligence) and their applications and trends in information management	2-basic	4-advanced 3-working	5-expert 4-advanced 3-working		2			5	6	
29. Image systems storage (micrographics) including filming, configurations, quality control, hardware, computer output microfilm, film testing, software, and storage	2-basic 1-limited	4-advanced 3-working	5-expert 4-advanced 3-working		2	3			6	

APPENDIX E

Occupational & Technical Knowledge & Skills	Complexity Level by Seniority			Relevant to CWFs						
	Entry	Journeyman	Senior							
30. Media and equipment transportation policies including USPS regulations and transportation requirements for non-postal service carriers (e.g., government and federal courier agencies)	2-basic	4-advanced	5-expert		2	3			6	
31. Electronic, optical, and other energy transfer of information (e.g., laser, fax, email, and web pages) policies and requirements	2-basic	4-advanced 3-working	5-expert		2	3			6	
32. Classification management and other protected information concepts and terms (including concepts and principles of original and derivative classification)	2-basic	4-advanced	5-expert	1	2	3			6	
33. Equity recognition, decision support, and appeals	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3			6	
34. Redaction techniques and processes	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3			6	
35. National disclosure policies	2-basic	4-advanced	5-expert	1	2	3		5	6	
36. Protection principles associated with human knowledge	2-basic	4-advanced	5-expert	1	2				6	
37. Failure analysis concepts, methods, principles, and techniques	2-basic	4-advanced	5-expert	1			4		6	
38. Development, preparation, and execution of information security presentations and briefings	2-basic	4-advanced	5-expert				4		6	7

APPENDIX F

SKILL STANDARDS FOR THE INFORMATION SYSTEMS SECURITY DISCIPLINE

SKILL STANDARDS FOR THE INFORMATION SYSTEMS SECURITY DISCIPLINE

OVERVIEW

This appendix contains skill standards for the Information Systems Security (ISS) discipline. It is important to understand skill standards terminology, abbreviations, and what the skill standards are before using this appendix. Appendix C, *Skill Standards Overview for Users of Appendices D-J*, describes the skill standards in detail. Carefully review Appendix C before using this appendix.

The content of this appendix consists of:

- Subject-Matter Expert Notes
- Skill Standard F-1: Information Systems Security Taxonomy
- Skill Standard F-2: Knowledge and Performance Levels Required on KAs in Relation to Seniority Level for Information Systems Security
- Skill Standard F-3: A&E K&S Importance by Seniority and Relevant CWFs for Information Systems Security
- Skill Standard F-4: Complexity Level by Seniority and Relevant CWFs for OTKS for Information Systems Security

SUBJECT-MATTER EXPERT NOTES

SMEs who contributed to the development of ISS skill standards attached three explanatory notes to the standards and also a formal definition of ISS as they were using the term. The SME notes and definition are presented verbatim below.

- Note 1: Information Systems Security (ISS) is one of seven separate and discrete security disciplines, which requires a select set of skill standards. In practice, it incorporates elements of the other six security disciplines: physical, personnel, information, communications, investigations and security management.
- Note 2: ISS is the implementation of measures that protect and defend information systems. These measures are collectively known as Information Assurance (IA).
- Note 3: ISS, as defined below, is an expansion of the definition listed in the Committee on National Security Systems (CNSS) Instruction No. 4009 as revised in May 2003.
- Study Definition of *Information Systems Security*: The protection of information systems against unauthorized access to the modification of information, whether in storage, processing or transit and against the denial of service to unauthorized users, including those measures necessary to detect, document and counter such threats. This includes the protective elements of physical

security, personnel security, information security, communications security, investigations, and security management.

Skill Standard F-1
Information Systems Security Taxonomy

CWF1: Evaluate new or current system(s) and security architectures

- KA1: Survey operational mission and uses
  - Mission objectives and operational imperatives are reviewed
  - Scope of operations is reviewed and assessed
  - Organization's security architecture applicability is reviewed
  - Information systems and security architecture are identified and/or reviewed
  - Current/planned uses, including system criticality, are assessed
  - Security supportability is assessed
- KA2: Evaluate levels of sensitive information
  - Sensitivity of the protected information, including any compartmented or special categories, is determined
  - Applicable access/exposure restrictions (i.e., need to know) are determined
  - Protection levels or category requirements are determined
- KA3: Identify sensitive access control requirements
  - Personnel access requirements are reviewed
  - Type of access (e.g., read, write, print) is verified
  - Current access methodologies are identified and assessed
- KA4: Determine applicable standards
  - Entities that have jurisdiction over information systems are determined
  - Legal and regulatory interventions are reviewed to determine applicability
  - Applicable information systems policies, standards, and procedures are identified
  - Information system security program history and documentation are reviewed

CWF2: Develop/update system security plan and training

- KA5: Determine information system boundary
  - Information system infrastructure is defined
  - Operating systems and software inventory are identified
  - Media access control and data transfer processes are determine
  - Personnel responsible for system management are identified
  - Information system's certification and accreditation status is determined
- KA6: Facilitate the development of contingency and disaster recovery plans
  - Contingency and disaster recovery requirements are reviewed
  - Existing emergency response policy, procedures, and plans are reviewed and/or updated
  - Back-up and restoration plans for hardware, software, data, and system connectivity are reviewed
- KA7: Determine and/or incorporate configuration change management processes
  - System operating policies and procedures are established
  - Information system's change control process' tracking of overarching changes impacting security is ensured
  - Information system's change control process is documented
  - Past instances of insecurities with similar configurations are reviewed
  - The security impact of maintenance practices is evaluated
- KA8: Perform preliminary risk assessment
  - Prior information systems security risk assessments and audits are reviewed
  - Known security vulnerabilities are reviewed
  - Risk elements that must be addressed in the security plan are determined
  - Appropriate risk mitigation strategies are determined
- KA9: Facilitate development/update of information system security plan(s)
  - Facilitation/participation in the plan development is ensured
  - Appropriate operational security (OPSEC) considerations are determined

  - Desktop compliance review of the plan is conducted
  - Information system security plan is processed for appropriate certification(s)
  - Incorporation of appropriate physical, personnel, information, and technical security considerations are ensured
- KA10: Plan information system security training
  - System specific training needs are determined
  - Options and resources required are determined
  - Options to meet ISS training program needs within subject organization are assessed

CWF3: Implement system security plan(s)

- KA11: Initiate certification process
  - System compliance with requirements is evaluated
  - Security test and evaluation of system is coordinated and monitored
  - Applicable system certification processes (e.g., AISSP, SSAA, MOU) are determined
  - Hardware vulnerabilities are identified
  - Results of certification testing (e.g., penetration testing, port scanning, DumpSec, COPS) are reviewed for security implications
  - Development of security certification report is coordinated
  - System changes that can affect its certification status is monitored
  - Corrective action plans are developed, if necessary
- KA12: Initiate accreditation process
  - Submission of certification documentation for accreditation is ensured
  - Accreditation status is monitored
  - Security aspects of identified corrective action areas are addressed
  - Correction action plan(s) are developed
- KA13: Implement information system security training
  - System-specific training is implemented
  - System user training completion is monitored and tracked
  - Training is reassessed and updated, as required

CWF4: Monitor compliance with system security plan(s)

- KA14: Monitor configuration compliance and changes to system security controls
  - Implementation of security controls within the system is monitored
  - Compliance with baseline system security configuration is monitored
  - Process describing changes to the system security configuration, including hardware and software, is monitored
  - Applicable Memorandums of Agreement and/or Understanding (MOA, MOU) are reviewed and monitored
  - Completed information system security risk assessments are reviewed
  - Impact of physical, personnel, information, and technical security changes is determined
  - User access privileges are reviewed
  - Systems' media controls and data transfer processes are monitored
  - Network connection rules and compliance are monitored
- KA15: Ensure auditing programs are in place
  - Information system security audit program is assessed
  - Activities of internal/external auditors are monitored
  - Audit reporting history is reviewed
- KA16: Perform periodic compliance reviews
  - Hardware/software baseline comparisons are conducted
  - Configurations, standards, policies, procedures, and instructions are assessed
  - Security plan currency with respect to policy is ensured
  - Need for re-accreditation is evaluated
  - Disposition activities are monitored

CWF5: Handle security deviations/violations

- KA17: Review known and past instances of insecurities
  - Past instances of loss, compromise, and suspected compromise of system information are evaluated

  - Approaches used to address past insecurities are reviewed
  - Actions taken to correct deficient policies/procedures are evaluated
- KA18: Apply existing policies and authorities regarding incident handling
  - Applicable policies and authorities are determined
  - Severity and type of incident are determined
  - Actions to be pursued and reporting requirements are determined
  - Requirements for assistance are identified (e.g., forensics, evidence trails, investigations)
  - Record keeping requirements are determined
  - Mitigation strategies are determined
- KA19: Ensure system users are trained on incident reporting procedures
  - Current training plans and requirements are reviewed
  - Compliance with training requirements are reviewed
  - Reporting deficiencies are reviewed

Skill Standard F-2
Knowledge and Performance Levels Required on KAs in Relation to Seniority Level for Information Systems Security

Key Activity	Knowledge Level by Seniority			Performance Level by Seniority		
	Entry	Journeyman	Senior	Entry	Journeyman	Senior
1. Survey operational mission and uses	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
2. Evaluate levels of sensitive information	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
3. Identify sensitive access control requirements	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
4. Determine applicable standards	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	2-partial	3-competent	3-competent
5. Determine information system boundary	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
6. Facilitate the development of contingency and disaster recovery plans	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
7. Determine and/or incorporate configuration change management processes	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
8. Perform preliminary risk assessment	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
9. Facilitate development/update of information system security plan(s)	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
10. Plan information system security training	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
11. Initiate certification process	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	2-partial	3-competent	3-competent
12. Initiate accreditation process	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	2-partial	3-competent	3-competent
13. Implement information system security training	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high

Key Activity	Knowledge Level by Seniority			Performance Level by Seniority		
	Entry	Journeyman	Senior	Entry	Journeyman	Senior
14. Monitor configuration compliance and changes to system security controls	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
15. Ensure auditing programs are in place	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	2-partial	3-competent	3-competent
16. Perform periodic compliance reviews	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	2-partial	3-competent	3-competent
17. Review known and past instances of insecurities	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
18. Apply existing policies and authorities regarding incident handling	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
19. Ensure system users are trained on incident reporting procedures	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	2-partial	3-competent	3-competent

Skill Standard F-3
A&E K&S Importance by Seniority and
Relevant CWFs for Information Systems Security

Academic & Employability Knowledge & Skills	Importance by Seniority			Relevant CWFs				
	Entry	Journeyman	Senior	1	2	3	4	5
1. Ability to Learn—Recognize and use learning techniques and recall available information to apply and adapt new knowledge and skills in both familiar and changing situations. Use multiple approaches when learning new things. Assess how one is doing when learning or doing something. Keep up to date technically and know one's own job and related jobs.	●	●	●	1	2	3	4	5
2. Adaptability—Change one's own behavior or work methods to adjust to other people or to changing situations or work demands; be receptive to new information, ideas or strategies to achieve goals.	●	●	●	1	2	3	4	5
3. Analyzing and Solving Problems—Anticipate or identify problems and their causes; develop and analyze potential solutions or improvements using rational and logical processes or innovations and creative approaches when needed.	●	●	●	1	2	3	4	5
4. Building Consensus—Build consensus among individuals or groups by facilitating agreements that involve sharing or exchanging resources or resolving difference in such a way as to promote mutual goals and interest; by persuading others to change their points of view or behavior without losing their future support; and by resolving conflicts, confrontation, and disagreements while maintaining productive working relationships.	●	●	●	1	2	3	4	5
5. Gathering and Analyzing Information—Obtain facts, information or data relevant to a particular problem, question or idea through observation of events or situations, discussions with others, or research or retrieval from written or electronic sources; organize, integrate, analyze and evaluate information.	●	●	●	1	2	3	4	5
6. Initiative/Motivation—Exert a high level of effort and perseverance towards goal attainment. Work hard to become excellent at doing tasks by setting high standards, paying attention to details, working well and displaying a high level of concentration even when assigned an unpleasant task. Display high standards of attendance, punctuality, enthusiasm, vitality and optimism in approaching and completing tasks. Demonstrate willingness to take on responsibilities and challenges and do what is needed without being asked.	●	●	●	1	2	3	4	5
7. Integrity/Honesty—Demonstrate dependability, conscientiousness, integrity and accountability. Show commitment to doing the job carefully and correctly. Fulfill obligations and be reliable, responsible and trustworthy. Perform tasks thoroughly and completely. Demonstrate honesty and avoidance of unethical behavior.	●	●	●	1	2	3	4	5
8. Leading Others—Motivate, inspire, and influence others toward effective individual or teamwork performance, goal attainment, and personal learning and development by serving as a mentor, coach and role model and by providing feedback and recognition or rewards.	n/a	●	●	1	2	3	4	5
9. Listening—Attend to, receive and correctly interpret verbal communications and directions through cues such as the content and context of the message and the tone, gesture and facial expression of the speaker.	●	●	●	1	2	3	4	5
10. Maintain Professional Demeanor—Demonstrate credibility and authority in issuing instructions and making requests to individuals and in performing duties. Maintains firm and direct tone of voice, authoritative posture, manner and bearing.	●	●	●	1	2	3	4	5

11. Making Decisions and Judgments—Make decisions that consider relevant facts and information, potential risks and benefits, and short- and long-term consequences or alternatives.	●	●	●	1	2	3	4	5
12. Mathematics—Understand, interpret and manipulate numeric or symbolic information; solve problems by selecting and applying appropriate quantitative methods such as arithmetic and estimation.	n/a	n/a	n/a					
13. Organizing and Planning—Organize and structure work for effective performance and goal attainment; set and balance priorities; anticipate obstacles; formulate plans consistent with available human, financial, and physical resources; modify plans or adjust priorities given changing goals or conditions.	●	●	●	1	2	3	4	5
14. Reading—Understand and use written information that may be presented in a variety of formats, such as text, tables, lists, figures, and diagrams; select reading strategies appropriate to the purpose, such as skimming for highlights, reading for detail, reading for meaning and critical analysis.	●	●	●	1	2	3	4	5
15. Science—Understand and apply the basic principles of physical, chemical, biological and earth sciences, understand and apply the scientific method, including formulating and stating hypotheses and evaluating them by experimentation or observation.	n/a	n/a	n/a					
16. Self and Career Development—Identify own work and career interests, strengths and limitations; pursue education, training, feedback or other opportunities for learning and development; manage, direct and monitor one's own learning and development.	n/a	n/a	n/a					
17. Speaking—Express ideas and facts orally in a clear and understandable manner that sustains listener attention and interest; tailor oral communications to the intended purpose and audience.	●	●	●	1	2	3	4	5
18. Stress Tolerance—Demonstrate maturity, poise and restraint to cope with pressure, stress, criticism, setbacks, personal and work-related problems, etc. Maintain composure, keeping emotions in check, controlling anger, and avoiding aggressive behavior even in very difficult situations. Accept criticism and deal calmly and effectively with high-stress situations.	●	●	●	1	2	3	4	5
19. Using Information and Communications Technology—Select, access and use necessary information, data, and communications-related technologies, such as basic personal computer applications, telecommunications equipment, Internet, electronic calculators, voice mail, email, facsimile machines and copying equipment to accomplish work activities.	●	●	●	1	2	3	4	5
20. Using Interpersonal Skills—Interact with others in ways that are friendly, courteous and tactful and that demonstrate respect for individual and cultural differences and for the attitudes and feelings of others.	●	●	●	1	2	3	4	5
21. Visual Observation—Notice details and take in and recall incoming visual sensory information and use it to make predictions, comparisons and/or evaluations. Recognize differences or similarities, or sensing changes in circumstances or events; discern between relevant visual cues or information and irrelevant or distracting information.	●	●	●	1	2	3	4	5
22. Working in Teams—Work cooperatively and collaboratively with others to achieve goals by sharing or integrating ideas, knowledge, skills, information, support, resources, responsibility and recognition.	●	●	●	1	2	3	4	5
23. Writing—Express ideas and information in written form clearly, succinctly, accurately, and in an organized manner; use English language conventions or spelling, punctuation, grammar, and sentence and paragraph structure; and tailor written communication to the intended purpose and audience.	●	●	●	1	2	3	4	5

Skill Standard F-4
Complexity Level by Seniority and Relevant CWFs
for OTKS for Information Systems Security

Occupational & Technical Knowledge & Skills	Complexity Level by Seniority			Revelant to CWFs				
	Entry	Journeyman	Senior					
1. Laws and Regulations Federal govt.-wide and organization-specific laws, regulations policies, guidelines, standards, and procedures mandating requirements for the management and protection of information technology resources. • Federal Laws and Regulations • Federal Standards and Guidelines • Legal and Liability Issues • Organization Policy, Guidelines, Standards, and Procedures Development • Organization Program • Issue-specific • System-specific	2-basic	3-working	4-advanced	1	2	3	4	5
2. IT Security Program A program established, implemented, and maintained to assure that adequate IT security is provided for all organizational information collected, processed, transmitted, stored, or disseminated in its general support systems and major applications. • Organization-wide IT Security Program • System-level IT Security Program • Elements of IT Security Program • Roles, Responsibilities, and Accountability o Senior Management o Organization-wide IT Security Mgrs. o Program and Functional Mgrs. o System/Application Owners o Information Owner/Custodian o IT System Security Mgrs. o Contractors o Related Security Program Mgrs o Users	2-basic	3-working	5-expert	1	2	3	4	5

Occupational & Technical Knowledge & Skills	Complexity Level by Seniority			Revelant to CWFs				
	Entry	Journeyman	Senior					
3. System Environment The unique technical and operating characteristics of an IT system and its associated environment, including the hardware, software, firmware, communications capability, and physical location. • IT Architecture • Hardware types • Operating software • Application software • Communication requirements • Facilities planning • Processing workflow • Utility software • Associated threats • Associated vulnerabilities	2-basic	3-working	5-expert	1	2	3	4	5
4. System Interconnection The requirements for communication or interconnection by an IT system with one or more other IT systems or networks, to share processing capability or pass data and information in support of multi-organizational or public programs. • Communications Types • Network Architecture • Electronic Mail • Electronic Commerce o EFT o Electronic Data Interchange o Digital Signatures o Electronic Signatures • Access Controls (e.g., firewalls, proxy servers, dedicated circuits) • Monitoring • Cryptography	2-basic	3-working	5-expert	1	2	3	4	5

Occupational & Technical Knowledge & Skills	Complexity Level by Seniority			Revelant to CWFs				
	Entry	Journeyman	Senior					
5. Information Sharing The requirements for information sharing by an IT system with one or more other IT systems or applications, for information sharing to support multiple internal or external organizations, missions, or public programs. • Communications Types • Network Architecture • Electronic Mail • Electronic Commerce o EFT o Electronic Data Interchange o Digital Signatures o Electronic Signatures • Access Controls (e.g., firewalls, proxy servers, dedicated circuits) • Monitoring • Cryptography • Data Ownership • Protection and Labeling of Data Storage Media	2-basic	3-working	5-expert	1	2	3	4	5
6. Sensitivity An IT environment consists of the system, data, and applications which must be examined individually and in toral. All IT systems and applications require some level of protection which is determined by an evaluation of the sensitivity and criticality of the information processed, the relation of the system to the organization missions and the economic value of the system components • Confidentiality • Integrity • Availability • Criticality • Aggregation	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4	5

Occupational & Technical Knowledge & Skills	Complexity Level by Seniority			Revelant to CWFs				
	Entry	Journeyman	Senior					
7. Risk Management The ongoing process of assessing the risk to IT resources and information, as part of a risk-based approach used to determine adequate security for a system, by analyzing the threats and vulnerabilities and selecting appropriate cost-effective controls to achieve and maintain an acceptable level of risk. • Risk Assessment, Analysis, Mitigation • Uncertainty Analysis • Threats, Vulnerabilities, Risks • Probability Estimation • Rate of Occurrence • Asset Valuation • Adequate and Appropriate Protection of Assets • Cost Effectiveness • Cost-Benefit Analysis • Application Security Reviews/Audits • Verification Reviews • Internal Control Reviews • EDP Audits	2-basic	3-working	5-expert	1	2	3	4	5

Occupational & Technical Knowledge & Skills	Complexity Level by Seniority			Revelant to CWFs				
	Entry	Journeyman	Senior					
8. Management Controls Actions taken to manage the development, maintenance, and use of the system, including system-specific policies, procedures, and rules of behavior, individual roles and responsibilities, individual accountability and personnel security decisions • System/Application Responsibilities o Program and Functional Mgrs o Owners and Custodians o Contractors o Related Security Program Mgrs o IT System Security Mgr o Users • System/Application-Specific Policies and Procedures • Standard Operating Procedures • Personnel Security o Background Investigations o Position Sensitivity o Separation of Duties and Compartmentalizations • System Rules of Behavior o Assignment/Limitation of System Privileges o Connection to Other Systems and Networks o Intellectual Property/Copyright o Remote Access o Official vs. Unofficial System Use o Individual Accountability • Sanctions or Penalties for Violations	2-basic	3-working	5-expert	1	2	3	4	5

Occupational & Technical Knowledge & Skills	Complexity Level by Seniority			Revelant to CWFs				
	Entry	Journeyman	Senior					
9. Acquisition/Development/Installation/ Implementation Controls The process of assuring that adequate controls are considered, evaluated, selected, designed and built into the system during its early planning and development stages and that an on-going process is established to ensure continued operation at an acceptable level of risk during the installation, implementation, and operation stages. • Life Cycle Planning • Security Activities in Life Cycle Stages • Security Plan Development and Maintenance • Security Specifications • Configuration Management • Change Control Procedures • Design Review and Testing • Authority to Operate o Certification/Recertification o Accreditation/Re-accreditation • Acquisition Specifications • Contracts, Agreements, and Other Obligations • Acceptance Testing • Prototyping	2-basic	3-working	5-expert	1	2	3	4	

Occupational & Technical Knowledge & Skills	Complexity Level by Seniority			Revelant to CWFs				
	Entry	Journeyman	Senior					
10. Operational Controls The day-to-day procedures and mechanisms used to protect operational systems and applications. Operational controls affect the system and application environment. • Physical and Environmental Proetection o Physical Security Program o Environmental Controls o Natural Threats o Facility Management o Fire Prevention and Protection o Electrical/Power o Housekeeping o Physical Access Controls o Intrusion Detection/Alarms o Maintenance o Water Plumbing o Mobile and Portable Systems • Production, Input/Output Controls o Document Labeling, Handling & Storing o Media Labeling, Handling & Storing o Disposal of Sensitive Material o Magnetic Remnance • Contingency Planning o Backups o Contingency/Disaster Recovery Plan Development, Testing, & Contracting • Audit and Variance Detection o System Logs and Records o Deviations from Standard Activity • Hardware and Software Maintenance Controls • Application Software Maintenance Controls • Documentation	2-basic	4-advanced	5-expert	1	2	3	4	5

Occupational & Technical Knowledge & Skills	Complexity Level by Seniority			Revelant to CWFs				
	Entry	Journeyman	Senior					
11. Awareness, Training, and Education Controls Awareness programs set the stage for training by changing organizational attitudes to realize the importance of security and the adverse consequences of its failure. Training teaches people the skills that will enable them to perform their jobs more effectively. Education is targeted for IT security professionals and focuses on developing the ability and vision to perform complex, multi-disciplinary activities.	2-basic	3-working	4-advanced	1	2	3	4	5

Occupational & Technical Knowledge & Skills	Complexity Level by Seniority			Revelant to CWFs				
	Entry	Journeyman	Senior					
12. Technical Controls Consist of hardware and software controls used to provide automated protection to the IT system or applications. Technical controls operate within the technical system and applications. • User Identification and Authentications o Passwords, Tokens, Biometrics, Single Log-In • Authorization/Access Controls o Logical Access Controls o Role-Based Access o System/Application Privileges • Integrity/Validation Controls o Compliance with Security Specifications and Requirements o Malicious Program/Virus Protection, Detection, and Removal o Authentication Messages o Reconciliation Routines • Audit Trail Mechanisms o Transaction Monitoring o Reconstruction of Transactions • Confidentiality controls o Cryptography • Incident Response o Fraud, Waste or Abuse o Hackers and Unauthorized User Activities o Incident Reporting and Investigation o Prosecution • Public Access Controls o Access Controls o Need-to-know and Privileges • Control Objectives and Protection Requirements	2-basic	4-advanced	5-expert	1	2	3	4	5

APPENDIX G

SKILL STANDARDS FOR THE PERSONNEL SECURITY DISCIPLINE

SKILL STANDARDS FOR THE PERSONNEL SECURITY DISCIPLINE

OVERVIEW

This appendix contains skill standards for the Personnel Security discipline. It is important to understand skill standards terminology, abbreviations, and what the skill standards are before using this appendix. Appendix C, *Skill Standards Overview for Users of Appendices D-J*, describes the skill standards in detail. Carefully review Appendix C before using this appendix.

The content of this appendix consists of:

- Skill Standard G-1: Personnel Security Taxonomy
- Skill Standard G-2: Knowledge and Performance Levels Required on KAs in Relation to Seniority Level for Personnel Security
- Skill Standard G-3: A&E K&S Importance by Seniority and Relevant CWFs for Personnel Security
- Skill Standard G-4: Complexity Level by Seniority and Relevant CWFs for OTKS for Personnel Security

Skill Standard G-1
Personnel Security Taxonomy

CWF1: Define Personnel Security Standards

- KA1: Delineate Employment and Associational Requirements
  - “Employment” security standards are identified, defined, and monitored
  - Third-party contractor security standards are identified, defined, and monitored
  - Legal and regulatory constraints, if any, are identified, reviewed, and monitored
  - Program plans and/or processing requirements are developed
- KA2: Apply National Security Clearance and/or Specialized Access Requirements
  - Requirements and/or “specialized access” provisions are identified, defined, and monitored
  - Program objectives and processes are identified and developed
  - Legal and regulatory constraints, if any, are identified, reviewed, and monitored
  - Program plans and/or processing requirements are developed
- KA3: Apply Reliability and/or Suitability Concerns
  - High risk task elements requiring greater reliability and/or suitability concerns are identified, defined, and monitored
  - Participation in the determination and evaluation of job sensitivity designations are met
  - Program objectives and processes are identified, defined, and monitored
  - Legal and regulatory constraints, if any, are identified, reviewed, and monitored
  - Program plans and/or processing requirements are developed

CWF2: Define Additional Vendor and Contractor Standards

- KA4: Apply Qualification and Reliability Standards
  - Qualification and reliability standards are determined
  - Sources of relevant information are identified
  - Legal and regulatory constraints, if any, are identified, reviewed, and monitored
  - System to collect and evaluate necessary information is developed
  - Process to make determination and process to document and notify appropriate responsible authorities are defined
- KA5: Verify Applicable Conditions of Association
  - Conditions of association that require verification are determined
  - Dissemination requirements are defined
  - Most efficient way of verification is determined
  - Most efficient way to disseminate information is determined
- KA6: Monitor Conditions of Contractor Standards
  - Elements of contractor standards that require monitoring are determined
  - Restrictions on monitoring by affected organizations are determined
  - Self-reporting processes are evaluated
  - Documentation and dissemination requirements are defined

CWF3: Perform Background Investigation

- KA7: Plan background Investigation
  - Briefing guide is prepared
  - Work load is prioritized
  - Appointments are scheduled
  - Administrative duties are performed
  - Process to make determination and process to document and notify appropriate responsible authorities are defined
- KA8: Conduct background investigation
  - Record reviews are conducted
  - Source/Reference interviews are conducted
  - Subject interviews are conducted
  - Investigative issues are pursued
- KA9: Write report of investigation
  - Investigative process used is documented
  - Results of record reviews are documented

- Results of subject interviews are documented
- Results of source/reference interviews are documented

CWF4: Conduct Adjudication Activities

- KA10: Review case file
  - Case file is evaluated for completeness
  - Content of all documents are reviewed to identify issues
  - Processing of case is completed
- KA11: Apply adjudication standards
  - Security concerns are analyzed against adjudicative standards
  - Mitigators of concerns are identified and evaluated
  - Decision and/or recommendation is made using “whole person” concept
- KA12: Document decision and/or recommendation
  - Determination is documented
  - Appropriate personnel is notified of decision and/or recommendation
  - Case is appropriately closed
- KA13: Manage case/work load
  - Case/work load is prioritized
  - Accountability is ensured
  - Guidance and assistance is provided to others
  - Assistance in the development of standard operating procedures and agency specific policy is provided
  - Case assignments are reviewed

CWF5: Administer Visitor Access Control

- KA14: Establish Relationship Verifications
  - Verification authorities are identified
  - Processes for relationship verifications are identified, defined, and monitored
  - Documentation and dissemination requirements are defined
- KA15: Establish Personal Identification Verifications
  - Applicability standards and process for verification are determined
  - Documents deemed acceptable for verification are identified
  - Roles and responsibilities are established
  - Documentation and dissemination requirements are defined
- KA16: Establish Access Need and/or Status Verifications
  - Process for determining scope and level of access needs is identified
  - Roles and responsibilities are established
  - Documentation and notification needs and/or processes are defined
- KA17: Document and/or Verify Applicable Conditions of Entry
  - Conditions of entry are identified and established
  - Process and/or procedures to administer are developed
  - Documentation and dissemination requirements are defined
- KA18: Develop and Implement Monitoring Activities
  - Criticality of elements of visitor standards are determined
  - Elements that can be reasonably monitored are determined
  - A monitoring plan is developed and/or applied

CWF6: Establish Security Education and Training

- KA19: Define Program
  - Program needs are identified and evaluated
  - Legal, regulatory, executive order, and other requirements and constraints are identified, reviewed, and monitored
  - Program scope requirements, option, and needed resources are determined
  - Program plans and/or other processes are developed
- KA20: Determine Initial and/or Entry Training Requirements
  - Initial and/or entry organizational requirements, education and training needs are determined
  - Subject matter content are identified, defined, and monitored

  - Procedures to administer program are established
  - Documentation and/or notification needs are identified and/or established
- KA21: Determine Special Responsibilities and/or Duty Requirements
  - Special responsibilities and/or duty training requirements are determined
  - Subject matter content are identified, defined, and monitored
  - Procedures to administer program are established
  - Documentation and/or notification needs are identified and/or established
- KA22: Determine Special Occurrence and/or Advisory Requirements
  - Special occurrence and/or advisory training requirements are determined
  - Subject matter content are identified, defined, and monitored
  - Procedures to administer program are established
  - Documentation and/or notification needs are identified and/or established
- KA23: Conduct Continuing Security Awareness Training
  - Continuing security awareness requirements are determined
  - Subject matter content are identified, defined, and monitored
  - System to distribute changes and updates to subject matter content is developed
  - Procedures to administer program are established
  - Briefing and debriefing requirements are identified
  - Briefing and debriefing are conducted (note: appropriate closeout procedures must be followed)
  - Documentation and/or notification needs are identified and/or established and monitored

CWF7: Administer Personnel Security Files

- KA24: Administer Files
  - File content categories are defined
  - Content, location(s), dissemination, and/or procedural requirements are defined
  - Access control protocols and procedures are defined
  - File system security and/or protection needs are defined
  - Security, permanent record, privacy act, and freedom of information act restrictions (and other issues including consideration of legal and/or regulatory implications) are identified and monitored
  - Required or needed file systems are established
- KA25: Document Personal Identification
  - Acceptable information and/or documents are determined
  - Source of information and/or documents are determined
  - Verification protocols (including, but not limited to, biometric identification needs) are developed
  - Required identification documentation processes are established
  - Systems to monitor and update records are developed
- KA26: Process Personnel Security Questionnaires and Statements
  - Legal authority for collecting information is determined
  - Requisite information is determined
  - Appropriate questionnaires and certifications are identified, defined, and monitored
  - Supplemental release forms, etc. are identified, defined, and monitored
  - Subject reporting requirements are established
- KA27: Document Security Status
  - Applicable accesses, clearances, assurances, certifications, etc. are determined
  - Requisite forms (originals) are determined
  - Distribution requirements are determined
  - System to record, monitor, and disseminate change of status is developed
- KA28: Document Security Training
  - Security training that requires records is determined
  - Required dissemination of records is determined
  - System to collect and update records is developed
  - Records are analyzed to document identified training needs and/or requirements
- KA29: Process Personal Reports

  - Elements and/or conditions requiring submission of report are identified
  - Security, permanent record, privacy act, freedom of information act or other restrictions are identified
  - Processing, dissemination, and retention requirements are determined
  - Implementation plans and/or other processing procedures are developed
- KA30: Control and Protect Reports of Investigations (ROIs) and Adjudicative Products
  - Procedural requirements are defined
  - Process for obtaining ROIs or other information are identified
  - Dissemination and access standards are determined

CWF8: Perform Other Personnel Security Activities

- KA31: Handle Sensitive and Classified Personnel Security Information
  - Application of sensitive, information security, and other security requirements are ensured
  - Required restrictions and associated handling measures are observed
  - Advise regarding related restrictions or protective caveats are provided to others who receive investigative products
  - Compliance with disposition requirements is ensured
- KA32: Administer Badge and Pass Program
  - Program needs and/or desires are determined
  - Physical and personnel security element needs are evaluated and/or integrated
  - Legal and regulatory constraints, if any, are identified and reviewed
  - Program scope (employees, visitors, etc.) is determined
  - Program plan is developed
- KA33: Monitor and Document Security Performance
  - Critical personnel security performance elements are identified
  - Monitoring processes and options are identified
  - Legal and regulatory constraints, if any, are identified and reviewed
  - Implementation processes are developed
- KA34: Initiate Use of Polygraph, as appropriate
  - Polygraph requirements are identified
  - Organizational policy for polygraph use is determined
  - Legal and regulatory constraints, if any, are identified and reviewed
  - Sources for polygraph support are identified
  - Appropriate program plans are developed
- KA35: Conduct Counterintelligence Reviews
  - Need for counterintelligence organizational support is determined
  - Intelligence threat is assessed
  - Operational vulnerability to intelligence collection is assessed
  - Countermeasures plan is developed, implemented, and monitored
- KA36: Conduct Liaison with Internal And External Organizations
  - Independent judgments and discretion are exercised to effectively represent the organization's position to internal and external officials
  - Materials for presentations and briefings for use are developed, as required
  - Liaison activities are conducted with internal and external personnel (including governmental officials, contractor groups, and others), as required
  - Responses to internal and external contacts (for the exchange of information regarding personnel security matters) are made and/or arranged
  - Required or needed follow-up activities are conducted
- KA37: Evaluate Personnel Security Program Performance
  - Program goals are determined
  - Participation in the development of corresponding operating procedures and agency-specific policy formulation is met
  - Assessment criteria are developed
  - Program implementation plan is developed
  - Measurement criteria are developed

  - Evaluation is conducted
- KA38: Assess incident involvement
  - Record of incidents is identified and reviewed
  - Personnel involved are identified
  - Nature of personnel involvement is assessed and documented
  - Appropriate notification protocols are developed

Skill Standard G-2
Knowledge and Performance Levels Required on KAs in Relation to Seniority Level for Personnel Security

Key Activity	Knowledge Level by Seniority			Performance Level by Seniority		
	Entry	Journeyman	Senior	Entry	Journeyman	Senior
1. Delineate Employment and Associational Requirements	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
2. Apply National Security Clearance and/or Specialized Access Requirements	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
3. Apply Reliability and/or Suitability Concerns	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
4. Apply Qualification and Reliability Standards	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
5. Verify Applicable Conditions of Association	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
6. Monitor Conditions of Contractor Standards	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
7. Plan Background Investigation	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
8. Conduct Background Investigation	A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	1-limited	3-competent	4-high
9. Write Report of Investigation	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
10. Review Case File	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
11. Apply Adjudication Standards	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
12. Document Decision and/or Recommendation	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high

Key Activity	Knowledge Level by Seniority			Performance Level by Seniority		
	Entry	Journeyman	Senior	Entry	Journeyman	Senior
13. Manage case/work load	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
14. Establish Relationship Verifications	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
15. Establish Personal Identification Verifications	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
16. Establish Access Need and/or Status Verifications	A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	1-limited	3-competent	4-high
17. Document and/or Verify Applicable Conditions of Entry	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
18. Develop and Implement Monitoring Activities	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
19. Define Program	A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	1-limited	3-competent	4-high
20. Determine Initial and/or Entry Training Requirements	A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	1-limited	3-competent	4-high
21. Determine Special Responsibilities and/or Duty Requirements	A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	1-limited	3-competent	4-high
22. Determine Special Occurrence and/or Advisory Requirements	A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	1-limited	3-competent	4-high
23. Administer Files	A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	1-limited	3-competent	4-high
24. Document Personal Identification	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
25. Process Personnel Security Questionnaires and Statements	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high

Key Activity	Knowledge Level by Seniority			Performance Level by Seniority		
	Entry	Journeyman	Senior	Entry	Journeyman	Senior
26. Document Security Status	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
27. Document Security Training	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
28. Process Personal Reports	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
29. Control and Protect Reports of Investigations (ROIs) and Adjudicative Products	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
30. Handle Sensitive and Classified Personnel Security Information	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
31. Administer Badge and Pass Program	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
32. Monitor and Document Security Performance	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
33. Initiate Use of Polygraph, as appropriate	A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	1-limited	3-competent	4-high
34. Assess Incident Involvement	A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	1-limited	3-competent	4-high
35. Conduct Counterintelligence Reviews	A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	1-limited	3-competent	4-high
36. Conduct Liaison with Internal and External Organizations	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
37. Evaluate Personnel Security Program Performance	A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	1-limited	3-competent	4-high
38. Assess Incident Involvement	A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	1-limited	3-competent	4-high

Skill Standard G-3
A&E K&S Importance by Seniority and Relevant CWFs for Personnel Security

Academic & Employability Knowledge & Skills	Importance by Seniority			Relevant CWFs							
	Entry	Journeyman	Senior	1	2	3	4	5	6	7	8
1. Ability to Learn—Recognize and use learning techniques and recall available information to apply and adapt new knowledge and skills in both familiar and changing situations. Use multiple approaches when learning new things. Assess how one is doing when learning or doing something. Keep up to date technically and know one's own job and related jobs.	●	●	●	1	2	3	4	5	6	7	8
2. Adaptability—Change one's own behavior or work methods to adjust to other people or to changing situations or work demands; be receptive to new information, ideas or strategies to achieve goals.	●	●	●	1	2	3	4	5	6	7	8
3. Analyzing and Solving Problems—Anticipate or identify problems and their causes; develop and analyze potential solutions or improvements using rational and logical processes or innovations and creative approaches when needed.	●	●	●	1	2	3	4	5	6	7	8
4. Building Consensus—Build consensus among individuals or groups by facilitating agreements that involve sharing or exchanging resources or resolving difference in such a way as to promote mutual goals and interest; by persuading others to change their points of view or behavior without losing their future support; and by resolving conflicts, confrontation, and disagreements while maintaining productive working relationships.	n/a	●	●			3	4				
5. Gathering and Analyzing Information—Obtain facts, information or data relevant to a particular problem, question or idea through observation of events or situations, discussions with others, or research or retrieval from written or electronic sources; organize, integrate, analyze and evaluate information.	●	●	●	1	2	3	4	5	6	7	8
6. Initiative/Motivation—Exert a high level of effort and perseverance towards goal attainment. Work hard to become excellent at doing tasks by setting high standards, paying attention to details, working well and displaying a high level of concentration even when assigned an unpleasant task. Display high standards of attendance, punctuality, enthusiasm, vitality and optimism in approaching and completing tasks. Demonstrate willingness to take on responsibilities and challenges and do what is needed without being asked.	●	●	●	1	2	3	4	5	6	7	8
7. Integrity/Honesty—Demonstrate dependability, conscientiousness, integrity and accountability. Show commitment to doing the job carefully and correctly. Fulfill obligations and be reliable, responsible and trustworthy. Perform tasks thoroughly and completely. Demonstrate honesty and avoidance of unethical behavior.	●	●	●	1	2	3	4	5	6	7	8

Academic & Employability Knowledge & Skills	Importance by Seniority			Relevant CWFs							
	Entry	Journeyman	Senior	1	2	3	4	5	6	7	8
8. Leading Others—Motivate, inspire, and influence others toward effective individual or teamwork performance, goal attainment, and personal learning and development by serving as a mentor, coach and role model and by providing feedback and recognition or rewards.	n/a	●	●	1	2	3	4	5	6	7	8
9. Listening—Attend to, receive and correctly interpret verbal communications and directions through cues such as the content and context of the message and the tone, gesture and facial expression of the speaker.	●	●	●	1	2	3	4	5	6	7	8
10. Maintain Professional Demeanor—Demonstrate credibility and authority in issuing instructions and making requests to individuals and in performing duties. Maintains firm and direct tone of voice, authoritative posture, manner and bearing.	n/a	●	●	1	2	3	4	5	6	7	8
11. Making Decisions and Judgments—Make decisions that consider relevant facts and information, potential risks and benefits, and short- and long-term consequences or alternatives.	●	●	●	1	2	3	4	5	6	7	8
12. Mathematics—Understand, interpret and manipulate numeric or symbolic information; solve problems by selecting and applying appropriate quantitative methods such as arithmetic and estimation.	n/a	n/a	●	1	2	3	4	5	6	7	8
13. Organizing and Planning—Organize and structure work for effective performance and goal attainment; set and balance priorities; anticipate obstacles; formulate plans consistent with available human, financial, and physical resources; modify plans or adjust priorities given changing goals or conditions.	n/a	●	●	1	2	3	4	5	6	7	8
14. Reading—Understand and use written information that may be presented in a variety of formats, such as text, tables, lists, figures, and diagrams; select reading strategies appropriate to the purpose, such as skimming for highlights, reading for detail, reading for meaning and critical analysis.	●	●	●	1	2	3	4	5	6	7	8
15. Science—Understand and apply the basic principles of physical, chemical, biological and earth sciences, understand and apply the scientific method, including formulating and stating hypotheses and evaluating them by experimentation or observation.	n/a	n/a	n/a								
16. Self and Career Development—Identify own work and career interests, strengths and limitations; pursue education, training, feedback or other opportunities for learning and development; manage, direct and monitor one's own learning and development.	●	●	●	1	2	3	4	5	6	7	8
17. Speaking—Express ideas and facts orally in a clear and understandable manner that sustains listener attention and interest; tailor oral communications to the intended purpose and audience.	●	●	●	1	2	3	4	5	6	7	8

Academic & Employability Knowledge & Skills	Importance by Seniority			Relevant CWFs							
	Entry	Journeyman	Senior	1	2	3	4	5	6	7	8
18. Stress Tolerance—Demonstrate maturity, poise and restraint to cope with pressure, stress, criticism, setbacks, personal and work-related problems, etc. Maintain composure, keeping emotions in check, controlling anger, and avoiding aggressive behavior even in very difficult situations. Accept criticism and deal calmly and effectively with high-stress situations.	●	●	●	1	2	3	4	5	6	7	8
19. Using Information and Communications Technology—Select, access and use necessary information, data, and communications-related technologies, such as basic personal computer applications, telecommunications equipment, Internet, electronic calculators, voice mail, email, facsimile machines and copying equipment to accomplish work activities.	●	●	●	1	2	3	4	5	6	7	8
20. Using Interpersonal Skills—Interact with others in ways that are friendly, courteous and tactful and that demonstrate respect for individual and cultural differences and for the attitudes and feelings of others.	●	●	●	1	2	3	4	5	6	7	8
21. Visual Observation—Notice details and take in and recall incoming visual sensory information and use it to make predictions, comparisons and/or evaluations. Recognize differences or similarities, or sensing changes in circumstances or events; discern between relevant visual cues or information and irrelevant or distracting information.	●	●	●	1	2	3	4	5	6	7	8
22. Working in Teams—Work cooperatively and collaboratively with others to achieve goals by sharing or integrating ideas, knowledge, skills, information, support, resources, responsibility and recognition.	●	●	●	1	2	3	4	5	6	7	8
23. Writing—Express ideas and information in written form clearly, succinctly, accurately, and in an organized manner; use English language conventions or spelling, punctuation, grammar, and sentence and paragraph structure; and tailor written communication to the intended purpose and audience.	●	●	●	1	2	3	4	5	6	7	8

Skill Standard G-4
Complexity Level by Seniority and Relevant CWFs for OTKS for Personnel Security

Occupational & Technical Knowledge & Skills	Complexity Level by Seniority			Relevant to CWFs							
	Entry	Journeyman	Senior								
1. Policies, regulations, guidelines and ethical standards that govern the conduct of Personnel Security Investigations (including, but not limited to): • Investigative standards • Section 1001 and 1905, Title XVIII US Code and other applicable laws • DCID 6/4 • EO 12968 • EO 10450 • Privacy Act 1974 & Freedom of Information Act • Ethical standards (prohibitions and forbidden topics) • Other policies and directives	2-basic 1-limited	3-working	5-expert 4-advanced	1	2	3	4	5	6	7	8
2. Adjudicative guidelines • Allegiance to the United States • Foreign influence • Foreign preference • Sexual Behavior • Personal Conduct • Financial considerations • Alcohol consumption • Drug involvement • Emotional, mental, personality disorders • Criminal conduct • Security violations • Outside activities • Misuse of information technology systems	1-limited	3-working	5-expert	1		3	4	5	6	7	8
3. Investigation concepts, principles, and practices (including, but not limited to): • Types of investigations • Scope of investigations • Coverage requirements for each type of investigation (e.g., Single Scope Background Investigations (SSBI) and SSBI-Periodic Reinvestigations)	1-limited	4-advanced 3-working	5-expert 4-advanced	1		3	4	5	6	7	8
4. Case and time management strategies	2-basic 1-limited	4-advanced 3-working	5-expert 4-advanced	1	2	3	4	5	6	7	8

Occupational & Technical Knowledge & Skills	Complexity Level by Seniority			Relevant to CWFs							
	Entry	Journeyman	Senior								
5. Information elicitation techniques (including, but not limited to): • Policies regarding telephonic interviews • Handling requests for presence of representation during interviews	2-basic 1-limited	4-advanced 3-working	5-expert	1	2	3	4	5	6	7	8
6. Guidance regarding proper taking, use and handling of investigative notes	2-basic 1-limited	4-advanced 3-working	5-expert			3	4		6		8
7. Threat situation and their impact (including, but not limited to): • counter-intelligence and counter-terrorism • personal safety and environment	1-limited	4-advanced 3-working	5-expert 4-advanced			3		5			8
8. Concepts, principles, and practices of polygraph use	1-limited	3-working	5-expert 4-advanced			3	4	5		7	8
9. Case-related information regarding government and private organizations' functions and structure	2-basic 1-limited	4-advanced 3-working	5-expert 4-advanced			3	4				
10. Concepts, principles, and practices associated with standard reporting format	2-basic 1-limited	4-advanced 3-working	5-expert 4-advanced			3	4				
11. Types of sources	2-basic 1-limited	4-advanced 3-working	5-expert			3	4	5	6	7	
12. Concepts, principles, and practices associated with the application of adjudicative criteria, disqualifying factors, and mitigating factors	1-limited	4-advanced 3-working	5-expert	1	2	3	4				
13. Agency-specific terminology, structure, instructions, correspondence procedures, or regulations	1-limited	4-advanced 3-working	5-expert	1	2	3	4	5	6	7	8
14. Levels of clearance and access	3-working 2-basic 1-limited	4-advanced 3-working	5-expert	1	2	3	4	5	6	7	8
15. Interim access criteria and justifications	1-limited	4-advanced 3-working	5-expert	1	2		4	5	6	7	8

Occupational & Technical Knowledge & Skills	Complexity Level by Seniority			Relevant to CWFs							
	Entry	Journeyman	Senior								
16. Terminologies (including, but not limited to): • Medical/mental health terminology • Financial terminology • Legal terminology • Alcohol/Drug terminology • Criminal behavior terminology • Immigration and naturalization terminology	2-basic 1-limited	4-advanced 3-working	5-expert	1	2	3	4	5	6	7	8
17. Special Program case procedures (including, but not limited to): • Special Access programs	1-limited	3-working	5-expert	1	2	3	4	5	6	7	8
18. Physical security requirements associated with personnel security	1-limited	3-working	5-expert 4-advanced	1	2	3	4	5	6	7	8
19. Computer and information systems usage guidelines (including, but not limited to): • IT-based applications related to personnel security (proper use, rules and guidelines)	1-limited	4-advanced 3-working	5-expert	1	2	3	4	5	6	7	8
20. Concepts, principles, and practices of financial analysis	2-basic 1-limited	4-advanced 3-working	5-expert			3	4		6		8
21. Hostile countries and organizations	2-basic 1-limited	3-working	5-expert			3	4		6		8
22. Case processing procedures	1-limited	3-working	5-expert			3	4		6		8
23. Concepts and principles of clearance, access, reliability, suitability, and trustworthiness	1-limited	4-advanced 3-working	5-expert	1	2	3	4	5	6	7	8
24. Ethical issues associated with personnel security	2-basic 1-limited	4-advanced 3-working	5-expert	1	2	3	4	5	6	7	8
25. Concepts, principles, and practices of proper control of records	1-limited	4-advanced 3-working	5-expert			3	4		6	7	

Occupational & Technical Knowledge & Skills	Complexity Level by Seniority			Relevant to CWFs							
	Entry	Journeyman	Senior								
26. Third party release provisions	1-limited	3-working	5-expert	1	2	3	4	5	6	7	8
27. Risk management concepts, principles, and practices	1-limited	4-advanced 3-working	5-expert	1	2	3	4	5	6	7	8
28. Record management requirements as related to personnel security	1-limited	4-advanced 3-working	5-expert	1	2	3	4	5	6	7	8
29. Information Assurance requirements as related to personnel security	1-limited	4-advanced 3-working	5-expert 4-advanced	1	2	3	4	5	6	7	8
30. Information System Security requirements as related to personnel security	1-limited	4-advanced 3-working	5-expert 4-advanced	1	2	3	4	5	6	7	8
31. Operations Security Program requirements as related to personnel security	1-limited	4-advanced 3-working	5-expert 4-advanced	1	2	3	4	5	6	7	8
32. Personnel security-related funding, manpower requirements, and budgeting programs	1-limited	3-working 2-basic	5-expert 4-advanced		2				6		8
33. Communications Security Program requirements as related to personnel security	1-limited	3-working	5-expert 4-advanced						6	7	8
34. Personnel security regulations and processes including protected information status, determination, assessment procedures, security, marking, control, accountability, and safeguarding of records	1-limited	4-advanced 3-working	5-expert	1	2	3	4	5	6	7	8
35. Preparation, coordination, and execution of MOU, MOA, Interservice Support Agreements, and Service Level Agreements	1-limited	3-working	5-expert 4-advanced	1	2	3	4	5	6	7	8
36. Program evaluation concepts, methods, and techniques	1-limited	3-working	5-expert 4-advanced	1	2	3	4	5	6	7	8
37. National disclosure policies	2-basic 1-limited	4-advanced 3-working	5-expert	1	2	3	4	5	6	7	8

Occupational & Technical Knowledge & Skills	Complexity Level by Seniority			Relevant to CWFs							
	Entry	Journeyman	Senior								
38. Development, preparation, and execution of personnel security presentations and briefings	1-limited	4-advanced 3-working	5-expert			3	4		6		8
39. Development, preparation, and execution of personnel security plans	1-limited	3-working	5-expert	1	2			5	6	7	8
40. Development, preparation, and execution of personnel security policies and procedures	1-limited	3-working	5-expert	1		3	4		6		
41. Vital records concepts, principles, and practices	1-limited	3-working	5-expert			3	4		6	7	8
42. Design and development of personnel security training and instruction	1-limited	3-working 2-basic	5-expert 4-advanced			3	4		6		8
43. Methods for analyzing, organizing, compiling, and reporting personnel security data	1-limited	4-advanced 3-working	5-expert	1	2	3	4	5	6	7	8

APPENDIX H

SKILL STANDARDS FOR THE PHYSICAL SECURITY DISCIPLINE

SKILL STANDARDS FOR THE PHYSICAL SECURITY DISCIPLINE

OVERVIEW

This appendix contains skill standards for the Physical Security discipline. It is important to understand skill standards terminology, abbreviations, and what the skill standards are before using this appendix. Appendix C, *Skill Standards Overview for Users of Appendices D-J*, describes the skill standards in detail. Carefully review Appendix C before using this appendix.

The content of this appendix consists of:

- Skill Standard H-1: Physical Security Taxonomy
- Skill Standard H-2: Knowledge and Performance Levels Required on KAs in Relation to Seniority Level for Physical Security
- Skill Standard H-3: A&E K&S Importance by Seniority and Relevant CWFs for Physical Security
- Skill Standard H-4: Complexity Level by Seniority and Relevant CWFs for OTKS for Physical Security

Skill Standard H-1
Physical Security Taxonomy

CWF 1: Oversee physical security of facility

- KA1: Evaluate location, utilities, and Infrastructure
  - Site-specific security issues are identified
  - Complete risk assessment for facility location is performed
  - Location's operational history is reviewed and determinations made
  - Existing condition and location of utilities are identified
  - Legal jurisdictions and available emergency services are identified
  - Location's planned uses and activities are determined
  - Impact of location of utilities in relation to critical operations of the facility is determined
  - Responsibility for and impact of cutoff and startup are determined
- KA2: Assess perimeter defense
  - Legal property lines and areas of cognizance are determined
  - Condition of perimeter barriers is evaluated
  - Appropriateness of property postings (e.g., signs) are reviewed and advice provided
  - Perimeter control protocols are evaluated and recommendations provided
  - Defensive strategies (e.g., defense in depth, channeling, stand-off, and mutual support) are deployed and/or employed
  - Perimeter lighting (e.g., types and capabilities of lighting system) is evaluated
  - Options and rating with respect to types and placement of barriers are determined
- KA3: Assess security properties of design and engineering
  - Physical construction is assessed
  - Physical security requirements are integrated into building design and plans to assure adequate physical security protection are reviewed
  - Construction are reviewed and assessed prior to release
  - Protective attributes of structure are determined and vulnerabilities identified
  - Applicable protective measures are determined
- KA4: Address personnel access controls
  - Controlled space requirements are identified
  - Understanding of facility's operational needs for personnel access is developed
  - Requirements established through agreements are identified
  - Entrance/Exit control protocols are determined/recommended
  - Security policies, procedures, and processes for personnel access controls are developed and implemented
- KA5: Address vehicle access controls
  - Internal traffic patterns are determined
  - Facility vehicle process needs are reviewed
  - Deliveries, inspection, search, and vehicle control procedures are evaluated
  - Vehicle regulations are reviewed and operating rules established
  - Security policies, procedures, and processes for vehicle access controls are developed and implemented
- KA6: Address material access controls
  - Material access requirements are reviewed
  - Documentation associated with cargo and delivery are checked and evaluated
  - Vulnerabilities associated with materials/deliveries are determined
  - Procedures for loss prevention, material control, and associated reporting protocols are developed
  - Characteristics of possible delivery means of hazardous devices/material (including, but not limited to, chemical, biological, radiological, nuclear, explosives) are evaluated
- KA7: Evaluate monitoring, detection, notification, and automatic response systems
  - Operational and system needs are reviewed/determined
  - Applicable laws and regulations are identified and reviewed
  - Available technology, integration, system compatibility, and scalability options are identified and reviewed

    - Initial and ongoing training and maintenance/spare parts needs are identified (life cycle maintenance)
    - Response requirements and procedures are identified and reviewed
    - Cost and benefit analysis are performed
    - Appropriate systems are determined and recommended
    - Comprehensive implementation plan is developed
- KA8: Address internal facility controls
    - Type(s) of controls, location(s), and control options are identified
    - Impact of fire code requirements (e.g., NFPA Life Safety Code 101) is determined
    - Basic principles of fire behavior and fire prevention practices are applied
    - Operational needs are evaluated to include compartmental identification
    - Issues of unintended emanations are addressed
    - Internal control plan and budget are developed
    - Approved plan is implemented
- KA9: Coordinate emergency services
    - Facility emergency needs are identified
    - Available resources and mutual aid support requirements (including first responders) are identified
    - Role and responsibilities of facility during emergency situations are determined
    - Emergency Services Plan is developed
    - Principles and procedures for Recovery and Continuity of Operations (COOP) are applied

CWF 2: Coordinate law enforcement activities

- KA10: Determine jurisdictions
    - Legal, criminal justice, delimitation, and "other" jurisdiction and/or cognizance issues for the facility is identified
    - Supporting court system is identified
    - Supporting law enforcement organizations are identified
    - Other available law enforcement resources are identified
- KA11: Define roles and procedures
    - Authority and responsibility are defined
    - Capabilities are identified and defined
    - Availability and conditions of threat are determined
    - Procedures to activate use are defined
- KA12: Establish liaison protocols
    - Points of contacts are established
    - Liaison/use protocols are established
    - Trigger events are determined
- KA13: Establish mutual aid programs
    - Internal capabilities are determined and evaluated
    - Available external capabilities are determined
    - Conditions under which mutual aid are applicable are determined
    - Mutual aid protocols/agreements are established

CWF 3: Coordinate guard operations

- KA14: Assess fixed posts and roving patrols
    - Needs, duties, responsibilities, and options are determined and evaluated
    - Human factor issues are identified and evaluated
    - Posts and patrols are deployed using techniques and principles of placement and mutual support
    - Operational procedures and schedule are developed
- KA15: Determine response protocols
    - Response categories (e.g., initial and secondary) and their initiation are identified and determined
    - Responders' roles and responsibilities are defined
    - Equipment needs of responders are determined

-
  - Response protocols (using principles of maneuver, cover, and concealment) are defined
  - Response actions are documented
- KA16: Identify standards and training
  - Applicable laws, standards, regulations, policies, and requirements are identified
  - Training needs and methods of training delivery are determined
  - Special training needs (including WMD, blood borne pathogens, HAZMAT, First Aid/CPR) are determined
  - Training options/sources are identified
  - Program evaluation and monitoring protocols are determined
  - Operational training plan is developed and approval obtained
  - Training program is implemented and monitored
- KA17: Address use of force and weapons
  - Applicable laws, standards, regulations, policies, and requirements are identified
  - A “Use of Force” policy is evaluated and established
  - Escalation of force protocol is identified and established
  - Equipment/weapons options to support “Use of Force” policy are identified and evaluated
  - Appropriate equipment/weapons are selected
  - Training programs are developed and implemented
- KA18: Evaluate communications needs and requirements
  - Communication needs to accomplish mission are identified
  - Level of sensitivity of needed communications is determined
  - Applicable regulatory requirements/restrictions are identified
  - Communications support plan is developed and approval obtained
  - Feedback to operational elements are provided
- KA19: Perform recording, reporting and administrative activities
  - Methods for determining hours and shift schedules are identified
  - Applicable mandatory record requirements (including training records) are reviewed and implemented
  - Availability of daily orders is validated
  - Effectiveness of guard reports are ensured

CWF4: Oversee physical security of special security areas

- KA20: Assess needs for and of security rooms and areas
  - Critical assets requiring protection are identified
  - Applicable laws, standards, regulations, policies, and requirements are identified
  - Necessary security/operational certifications are defined
  - Access requirements to assets are determined
  - Asset use is evaluated
  - Need for internal secure areas is evaluated
  - Potential secure areas are identified
  - Sound Transmission Class (STC) Levels and methods of measurement are determined
  - Role of UL standards are determined
  - Construction techniques are analyzed
  - Appropriate plans and recommendations are made
  - Plans are appropriately exercised
- KA21: Assess needs for and of shelters and bunkers
  - Critical assets requiring enhanced hardening are identified
  - Applicable laws, standards, regulations, policies, and requirements are identified
  - Necessary security/operational certifications are defined
  - Need for shelters and bunkers is evaluated
  - Potential locations for shelters and bunkers are identified
  - Appropriate plans and recommendations are made
  - Plans are appropriately exercised
- KA22: Assess needs for and of vaults and containers
  - Critical assets requiring protection are identified

  - Applicable laws, standards, regulations, policies, and requirements are identified
  - Access requirements to assets are determined
  - Asset use are evaluated
  - Necessary security/operational certifications are defined
  - Need for vaults and containers is evaluated
  - Potential locations for vaults and containers are identified
  - Locks, key control, hardware, and associated procedures are inspected
  - Appropriate plans and recommendations are made
  - Plans are appropriately exercised
- KA23: Protect critical technology installations and infrastructures
  - Risks are identified, assessed, and managed
  - Technology-unique protection considerations are reviewed
  - Health safety issues are determined against protection issues
  - OPSEC physical protection requirements are reviewed
  - Existing agreements and standards are reviewed
  - Required protection protocols are reconciled with issues of cognizance
  - Appropriate plans and recommendations are made
  - Plans are appropriately exercised
- KA24: Address security programs related to physical security and law enforcement
  - Personnel security is addressed appropriately
  - Operations security is addressed appropriately
  - Information security is addressed appropriately
  - Technical security is addressed appropriately
  - Communications security is addressed appropriately
  - Automated information systems are addressed appropriately

CWF5: Coordinate antiterrorism activities

- KA25: Address needs for and of executive protection
  - Appropriate risk assessment is conducted
  - Operational requirements and desire for program is evaluated
  - Legal and regulatory interventions are identified and reviewed
  - Scope of program, options, and required resources are determined
  - Program plan is developed
  - Plans are appropriately exercised
- KA26: Address needs for and of antiterrorism/force protection/ countermeasures program
  - Operational need/desire for program is evaluated
  - Appropriate risk assessment is conducted
  - Appropriate legal and regulatory interventions are identified
  - Scope of program, options, and required resources are determined
  - A “Rules of Engagement” policy is evaluated and established
  - A “Use of Force” policy is evaluated and established
  - Program plan is developed
  - Plans are appropriately exercised
- KA27: Address needs for and of explosive ordinance disposal (EOD)
  - Operational need/desire for program is evaluated
  - Appropriate risk assessment is conducted
  - Legal and regulatory interventions are identified and reviewed
  - Scope of program, options, and required resources are determined
  - Program plan is developed
  - Bomb threat plan is reviewed and inspected
  - Plans are appropriately exercised
- KA28: Address needs for and of recovery and continuity of operations programs
  - Principles and procedures for Recovery and Continuity of Operations (COOP) are applied
  - Sufficiency of recovery protections are evaluated
  - Physical security procedures of recovery efforts are reviewed

  - Appropriate legal and regulatory interventions are identified
  - Program plan and procedures are developed
  - Appropriate training is conducted
  - Plans are appropriately exercised
- KA29: Perform risk assessment
  - Vulnerability assessments are conducted
  - Current physical security threats are identified and verified
  - Current threats are assessed against known and identified physical security vulnerabilities
  - Threat and intelligence information are evaluated
  - Appropriate plans and recommendations are made
  - Plans are appropriately exercised
- KA30: Address special considerations for WMD-related items (e.g., CBRNE)
  - Legal requirements for search and/or inspection are determined
  - Relevant protection levels are identified
  - Sufficiency of protections are reviewed
  - Appropriate plans and recommendations are made
  - Plans are appropriately exercised
- KA31: Address infrastructure security needs
  - Site-specific security issues are identified
  - Complete risk assessment for facility location is performed
  - Need for and of strongrooms for designated high-risk personnel is addressed
  - Impact of location of utilities in relation to critical operations of the facility is determined
  - Appropriate plans and recommendations are made
  - Plans are appropriately exercised

CWF6: Oversee other physical security operations

- KA32: Address needs for and of transportation escorts and couriers
  - Criticality and sensitivity of assets are determined
  - Appropriate risk assessment is conducted
  - Need/desire to move assets are identified and evaluated
  - Available methods and options are identified and evaluated
  - Appropriate legal and regulatory interventions are identified
  - Security plan to support the operational movement plan are developed
  - Plans are appropriately exercised
- KA33: Evaluate central control and monitoring centers
  - Overall operational objectives and results are identified and evaluated
  - Location and operational requirements are identified and evaluated
  - Roles and responsibilities in support of response plan are identified and evaluated
  - Operational capabilities are identified and evaluated
  - Control and monitoring systems are identified and evaluated
  - Applicable laws, regulations, and standards are identified
  - Assessment report and plan are developed
  - Plans are appropriately exercised
- KA34: Oversee K9 Operations
  - Operational requirements/desired uses are evaluated
  - Operational and resource plans are developed
  - Legal and regulatory interventions are identified and reviewed (including certification and recertification requirements)
  - Sources of capability are identified
  - Options to satisfy operational requirements/desired uses are identified
  - Plans are appropriately exercised
- KA35: Coordinate emergency and disaster response support
  - Roles and responsibilities are defined
  - Support capabilities are evaluated
  - Legal and regulatory interventions are identified and reviewed
  - Scope of support program and required resources are determined

  - Support operations plan are defined and developed
  - Plans are appropriately exercised
- KA36: Support incident/crime scene
  - Roles and responsibilities are defined
  - Legal and regulatory interventions are identified and reviewed
  - Scope of plan, options, and resources required are determined
  - Plan and procedures are developed
  - Appropriate training is conducted
  - Plans are appropriately exercised
- KA37: Address needs for and of drug and explosive detection program
  - Operational need/desire for program is evaluated
  - Appropriate risk assessment is conducted
  - Legal and regulatory interventions are identified and reviewed
  - Scope of program, options, and required resources are determined
  - Program plan is developed
  - Plans are appropriately exercised
- KA38: Address needs for and of Special Weapons and Tactics (SWAT) and/or Emergency Response Teams
  - Operational need/desire for program is evaluated
  - Appropriate risk assessment is conducted
  - Legal and regulatory interventions are identified and reviewed
  - Scope of program, options, and required resources are determined
  - Program plan is developed
  - Plans are appropriately exercised
- KA39: Protect arms, ammunition, and explosives
  - Scope of program, options, and required resources are determined
  - Roles and responsibilities are defined
  - Legal and regulatory interventions are identified and reviewed
  - Program plan is developed
  - Appropriate training is conducted
  - Plans are appropriately exercised
- KA40: Address needs for and of restoration program
  - Sufficiency of restoration protections are evaluated
  - Physical security procedures of recovery efforts are reviewed
  - Appropriate legal and regulatory interventions are identified
  - Program plan and procedures are developed
  - Appropriate training is conducted
  - Plans are appropriately exercised

CWF7: Perform administrative functions

- KA41: Administer training programs
  - Appropriate training programs are identified and planned
  - Future training requirements are determined
  - In-house employee training programs are developed
  - Appropriate training programs are conducted
- KA42: Administer budgets
  - Budgeting requirements are forecasted
  - Budget plans are developed
  - Budgets are monitored and controlled
  - Contracts are administered
- KA43: Administer programs
  - Contacting officer responsibilities for programs are performed
  - Contract expenditures are monitored and future requirements determined
  - A76 comparative analysis of government versus contract functional tasks is reviewed
  - Procedures to support security operations are determined
  - Scheduling function is performed

- KA44: Assess and manage risk
  - Assets are identified and prioritized
  - Threats to assets are identified and verified
  - Vulnerabilities are identified and assessed
  - Risks are determined
  - Plan to mitigate risks is developed
  - Management decisions are implemented
- KA45: Process deviations
  - Deviations are identified and clarified
  - Necessity for compensatory measures are evaluated if deviations are imposed
  - Deviations are processed for appropriate review
  - Deviations are submitted to the appropriate approval boards
- KA46: Provide briefings and reports of inspections, assessments, and/or reviews
  - Briefings, based on accumulated information, are created and presented
  - Reports to support press releases are prepared
  - Subject matter expertise is provided to others (e.g., to support development of general awareness training)

Skill Standard H-2
Knowledge and Performance Levels Required on KAs in Relation to Seniority Level for Physical Security

Key Activity	Knowledge Level by Seniority			Performance Level by Seniority		
	Entry	Journeyman	Senior	Entry	Journeyman	Senior
1. Evaluate location, utilities, and infrastructure	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
2. Assess perimeter defense	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
3. Assess security properties of design and engineering	A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
4. Address personnel access controls	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	4-high	4-high
5. Address vehicle access controls	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	3-competent
6. Address material access controls	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	3-competent
7. Evaluate monitoring, detection, and automatic response systems	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
8. Address internal facility controls	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
9. Coordinate emergency services	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	1-limited	3-competent	4-high
10. Determine jurisdictions	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
11. Define roles and procedures	A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	1-limited	3-competent	4-high
12. Establish liaison protocols	A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	1-limited	3-competent	4-high

Key Activity	Knowledge Level by Seniority			Performance Level by Seniority		
	Entry	Journeyman	Senior	Entry	Journeyman	Senior
13. Establish mutual aid program	A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	1-limited	3-competent	4-high
14. Assess fixed posts and roving patrols	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
15. Determine response protocols	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	1-limited	3-competent	4-high
16. Identify standards and training	A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	1-limited	3-competent	4-high
17. Address use of force and weapons	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	3-competent
18. Evaluate communications needs and requirements	A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
19. Perform recording, reporting, and administrative activities	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
20. Assess needs for and of security rooms and areas	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
21. Assess needs for and of shelters and bunkers	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	1-limited	3-competent	4-high
22. Assess needs for and of vaults and containers	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
23. Protect critical technology, installations, and infrastructure	A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	1-limited	3-competent	4-high
24. Address security programs related to physical security and law enforcement	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
25. Address needs for and of executive protection	A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	1-limited	3-competent	4-high

Key Activity	Knowledge Level by Seniority			Performance Level by Seniority		
	Entry	Journeyman	Senior	Entry	Journeyman	Senior
26. Address needs for and of antiterrorism/force protection/ countermeasures program	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
27. Address needs for and of explosive ordinance disposal (EOD)	A-nomenclature	C-principles B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	1-limited	3-competent	3-competent
28. Address needs for and of recovery and of continuation of operations programs	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	1-limited	3-competent	4-high
29. Perform risk assessment	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
30. Address special considerations for WMD-related items (CBRNE)	A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	1-limited	3-competent	4-high
31. Address infrastructure needs	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	1-limited	3-competent	4-high
32. Address needs for and of transportation escorts and couriers	A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	1-limited	3-competent	4-high
33. Evaluate central control and monitoring systems	A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	1-limited	3-competent	4-high
34. Oversee K9 operations	A-nomenclature	C-principles B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	1-limited	3-competent	3-competent
35. Coordinate emergency and disaster response support	A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	1-limited	3-competent	4-high
36. Support incident/crime scene	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	2-partial	3-competent	3-competent
37. Address needs for and of drug and explosive detection program	A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	1-limited	3-competent	4-high

Key Activity	Knowledge Level by Seniority			Performance Level by Seniority		
	Entry	Journeyman	Senior	Entry	Journeyman	Senior
38. Address needs for and of Special Weapons and Tactics (SWAT) and/or Emergency Response Teams	A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	1-limited	3-competent	3-competent
39. Protect arms, ammunition, and explosives	A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	1-limited	3-competent	4-high
40. Address need for and of restoration program	A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	1-limited	3-competent	4-high
41. Administer training programs	A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	1-limited	3-competent	3-competent
42. Manage budgets	A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	1-limited	3-competent	4-high
43. Manage programs	A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	1-limited	3-competent	4-high
44. Assess and manage risk	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	4-high	4-high
45. Process deviations	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	1-limited	3-competent	4-high
46. Provide briefings and reports of inspections, assessments, and/or reviews	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high

Skill Standard H-3
A&E K&S Importance by Seniority and Relevant CWFs for Physical Security

Academic & Employability Knowledge & Skills	Importance by Seniority			Relevant CWFs						
	Entry	Journeyman	Senior	1	2	3	4	5	6	7
1. Ability to Learn—Recognize and use learning techniques and recall available information to apply and adapt new knowledge and skills in both familiar and changing situations. Use multiple approaches when learning new things. Assess how one is doing when learning or doing something. Keep up to date technically and know one's own job and related jobs.	●	●	●	1	2	3	4	5	6	7
2. Adaptability—Change one's own behavior or work methods to adjust to other people or to changing situations or work demands; be receptive to new information, ideas or strategies to achieve goals.	●	●	●	1	2	3	4	5	6	7
3. Analyzing and Solving Problems—Anticipate or identify problems and their causes; develop and analyze potential solutions or improvements using rational and logical processes or innovations and creative approaches when needed.	●	●	●	1	2	3	4	5	6	7
4. Building Consensus—Build consensus among individuals or groups by facilitating agreements that involve sharing or exchanging resources or resolving difference in such a way as to promote mutual goals and interest; by persuading others to change their points of view or behavior without losing their future support; and by resolving conflicts, confrontation, and disagreements while maintaining productive working relationships.	n/a	●	●	1	2	3	4	5	6	7
5. Gathering and Analyzing Information—Obtain facts, information or data relevant to a particular problem, question or idea through observation of events or situations, discussions with others, or research or retrieval from written or electronic sources; organize, integrate, analyze and evaluate information.	●	●	●	1	2	3	4	5	6	7
6. Initiative/Motivation—Exert a high level of effort and perseverance towards goal attainment. Work hard to become excellent at doing tasks by setting high standards, paying attention to details, working well and displaying a high level of concentration even when assigned an unpleasant task. Display high standards of attendance, punctuality, enthusiasm, vitality and optimism in approaching and completing tasks. Demonstrate willingness to take on responsibilities and challenges and do what is needed without being asked.	●	●	●	1	2	3	4	5	6	7
7. Integrity/Honesty—Demonstrate dependability, conscientiousness, integrity and accountability. Show commitment to doing the job carefully and correctly. Fulfill obligations and be reliable, responsible and trustworthy. Perform tasks thoroughly and completely. Demonstrate honesty and avoidance of unethical behavior.	●	●	●	1	2	3	4	5	6	7
8. Leading Others—Motivate, inspire, and influence others toward effective individual or teamwork performance, goal attainment, and personal learning and development by serving as a mentor, coach and role model and by providing feedback and recognition or rewards.	n/a	●	●	1	2	3	4	5	6	7
9. Listening—Attend to, receive and correctly interpret verbal communications and directions through cues such as the content and context of the message and the tone, gesture and facial expression of the speaker.	●	●	●	1	2	3	4	5	6	7

Academic & Employability Knowledge & Skills	Importance by Seniority			Relevant CWFs						
	Entry	Journeyman	Senior	1	2	3	4	5	6	7
10. Maintain Professional Demeanor—Demonstrate credibility and authority in issuing instructions and making requests to individuals and in performing duties. Maintains firm and direct tone of voice, authoritative posture, manner and bearing.	●	●	●	1	2	3	4	5	6	7
11. Making Decisions and Judgments—Make decisions that consider relevant facts and information, potential risks and benefits, and short- and long-term consequences or alternatives.	●	●	●	1	2	3	4	5	6	7
12. Mathematics—Understand, interpret and manipulate numeric or symbolic information; solve problems by selecting and applying appropriate quantitative methods such as arithmetic and estimation.	n/a	●	●	1	2	3	4	5	6	7
13. Organizing and Planning—Organize and structure work for effective performance and goal attainment; set and balance priorities; anticipate obstacles; formulate plans consistent with available human, financial, and physical resources; modify plans or adjust priorities given changing goals or conditions.	●	●	●	1	2	3	4	5	6	7
14. Reading—Understand and use written information that may be presented in a variety of formats, such as text, tables, lists, figures, and diagrams; select reading strategies appropriate to the purpose, such as skimming for highlights, reading for detail, reading for meaning and critical analysis.	●	●	●	1	2	3	4	5	6	7
15. Science—Understand and apply the basic principles of physical, chemical, biological and earth sciences, understand and apply the scientific method, including formulating and stating hypotheses and evaluating them by experimentation or observation.	n/a	●	●	1	2	3	4	5	6	7
16. Self and Career Development—Identify own work and career interests, strengths and limitations; pursue education, training, feedback or other opportunities for learning and development; manage, direct and monitor one's own learning and development.	●	●	●	1	2	3	4	5	6	7
17. Speaking—Express ideas and facts orally in a clear and understandable manner that sustains listener attention and interest; tailor oral communications to the intended purpose and audience.	●	●	●	1	2	3	4	5	6	7
18. Stress Tolerance—Demonstrate maturity, poise and restraint to cope with pressure, stress, criticism, setbacks, personal and work-related problems, etc. Maintain composure, keeping emotions in check, controlling anger, and avoiding aggressive behavior even in very difficult situations. Accept criticism and deal calmly and effectively with high-stress situations.	●	●	●	1	2	3	4	5	6	7
19. Using Information and Communications Technology—Select, access and use necessary information, data, and communications-related technologies, such as basic personal computer applications, telecommunications equipment, Internet, electronic calculators, voice mail, email, facsimile machines and copying equipment to accomplish work activities.	●	●	●	1	2	3	4	5	6	7
20. Using Interpersonal Skills—Interact with others in ways that are friendly, courteous and tactful and that demonstrate respect for individual and cultural differences and for the attitudes and feelings of others.	●	●	●	1	2	3	4	5	6	7

Academic & Employability Knowledge & Skills	Importance by Seniority			Relevant CWFs						
	Entry	Journeyman	Senior	1	2	3	4	5	6	7
21. Visual Observation—Notice details and take in and recall incoming visual sensory information and use it to make predictions, comparisons and/or evaluations. Recognize differences or similarities, or sensing changes in circumstances or events; discern between relevant visual cues or information and irrelevant or distracting information.	●	●	●	1	2	3	4	5	6	7
22. Working in Teams—Work cooperatively and collaboratively with others to achieve goals by sharing or integrating ideas, knowledge, skills, information, support, resources, responsibility and recognition.	●	●	●	1	2	3	4	5	6	7
23. Writing—Express ideas and information in written form clearly, succinctly, accurately, and in an organized manner; use English language conventions or spelling, punctuation, grammar, and sentence and paragraph structure; and tailor written communication to the intended purpose and audience.	●	●	●	1	2	3	4	5	6	7

Skill Standard H-4
Complexity Level by Seniority and Relevant CWFs for OTKS for Physical Security

Occupational & Technical Knowledge & Skills	Complexity Level by Seniority			Relevant to CWFs						
	Entry	Journeyman	Senior							
1: Laws, regulations, concepts, principles, and technology related to physical security including, but not limited to: • Interpretation of legal documents • research processes and procedures • principles for determining physical security measures to support mission • principles for integrating physical security protocols to ensure appropriate level of protection • deviation, waiver, and/or exception concept • establishing location boundaries • concept of Continuity of Government (COG) oversight • Concept of operations (CONOP) for the specific site and/or mission regarding protective forces needed for operational personnel	2-basic	4-advanced	5-expert	1	2	3	4	5	6	7

Occupational & Technical Knowledge & Skills	Complexity Level by Seniority			Relevant to CWFs						
	Entry	Journeyman	Senior							
2: Developments and advances in security systems, methods, equipment, and techniques including, but not limited to: • security equipments, operations, and sources of options • evaluation of commercially available integrated systems • principles for establishing technical standards (e.g., STC-TEMPEST) • principles for defining technical security measures (e.g., IDS, CCTV, Guard Access Control) • concept of protection levels • technology types, levels and applications • C3I requirements (e.g., elements of facility construction and limitations, types of systems/equipment required) • development of plans and procedures to operate physical security-related systems • procedures for establishing a "3 level" (i.e., telephone, radio, RF) communication system • principles for establishing training and maintenance requirements to manage security system sustainability	2-basic	4- advanced	5- expert	1	2	3	4	5	6	7
3: Physical security regulations and procedures required to protect mission essential areas including, but not limited to: • principles for establishing operations/mission of special security areas • unique operational requirements of special security areas • principles for establishing inspection and certification processes associated with special security areas	2-basic	4- advanced	5- expert	1		3	4	5	6	
4: Interview and elicitation techniques	2-basic	3-working	4- advanced	1	2	3	4	5	6	7

Occupational & Technical Knowledge & Skills	Complexity Level by Seniority			Relevant to CWFs						
	Entry	Journeyman	Senior							
5: Physical security survey/inspection and technical site survey inspection techniques including, but not limited to: • physical security regulations for initiating inspections, assessments, and/or reviews • concepts, principles, and methods for determining effectiveness of security measures, operability, and performance testing • use and interpretation of analytical and software system data to evaluate and model facility security system	2-basic	4- advanced	5- expert	1	2	3	4	5	6	7
6: Multi-layered security systems involving access controls, barriers, protection devices, monitoring equipment, security forces, and intrusion detection equipment including, but not limited to: • barrier types, their protective capabilities, and security effectiveness • types of lighting, protective levels relative to lumens available, and power sources • concepts and principles of time and distance factors (i.e., deny, delay) • layered defense concept • procedures for employing/deploying IDS/surveillance equipment to facilitate detection and response based on layered defense concept • equipment, processes, and physical security measures to control access (technology integration) • authorized access to specific areas versus general access • use of monitoring and detection systems (e.g., IDS and CCTV)	2-basic	4- advanced	5- expert	1	2	3	4	5	6	7
7: Methods for effective presentation of physical security and law enforcement data including, but not limited to:	2-basic	3- working	4- advanced	1	2	3	4	5	6	7

Occupational & Technical Knowledge & Skills	Complexity Level by Seniority			Relevant to CWFs						
	Entry	Journeyman	Senior							
8: Risk analysis and vulnerability assessment techniques including, but not limited to: • principles and methods for assessing vulnerabilities • principles and methods for identifying and verifying physical security threats • principles and methods for assessing threats against physical security vulnerabilities • principles and methods for evaluating threat and intelligence information	2-basic	4- advanced	5- expert	1	2	3	4	5	6	7
9: Concepts, practices, and principles associated with recovery/restoration programs	2-basic	3- working	4- advanced				4	5		
10: Development, preparation, and execution of physical security policies and procedures	2-basic	4- advanced	5- expert	1	2	3	4	5	6	7
11: Concepts, principles, and practices related to crime prevention including, but not limited to: • crime prevention, property, and inventory control and how to develop security plans associated with them • methods for analyzing crime trends and statistical data	2-basic	3- working	4- advanced	1	2	3	4	5	6	7

Occupational & Technical Knowledge & Skills	Complexity Level by Seniority			Relevant to CWFs						
	Entry	Journeyman	Senior							
12: Development, preparation, and execution of physical security plans including, but not limited to: • operational impacts on physical security measures (e.g., sizing security areas against operational parameters and physical security requirements) • relationship between the logistical, operational, and mission-driven requirements of location and security protection measures • principles for developing and implementing response plans • COOP plans to specifically include capabilities and respective limitations • principles of how to determine level of command, control, communications, computer, and intelligence based on operational goals and objectives • program evaluation principles (e.g., collect data, define physical security parameters, acknowledge problems, advise corrections, and evaluate programs) • installation mobilization/deployment contingency plans, regulations, and procedures	2-basic	4- advanced	5- expert	1	2	3	4	5	6	

Occupational & Technical Knowledge & Skills	Complexity Level by Seniority			Relevant to CWFs						
	Entry	Journeyman	Senior							
13: Laws, regulations, concepts, principles, practices, and technology related to law enforcement operations including, but not limited to: • local, state, federal legal requirements and standards (including their implications on authority and jurisdictional limitations) • arrest powers and areas of cognizance • law and policies relative to arrest, detention, search, inspection, and use of force • local restrictions • laws and techniques of search, seizure, and the use of force • civil rights of individuals and the rights of suspects • laws, regulations, and procedures pertaining to the collection, preservation, and accountability of evidence • security concepts and procedures for vehicle movements and parking (e.g., traffic flow patterns, traffic control devices)	2-basic	3- working	4- advanced	1	2	3	4	5	6	7

Occupational & Technical Knowledge & Skills	Complexity Level by Seniority			Relevant to CWFs						
	Entry	Journeyman	Senior							
14: Laws, regulations, concepts, principles, practices, and technology related to security guard operations including, but not limited to: • principles associated with determining fixed posts and roving patrol needs, deployment, and response techniques, tactics and strategies • writing post and patrol orders • principles associated with determining and using individual and team guard force equipment • applying First Aid and CPR • using assigned weapons and intermediate force equipment (e.g., chemical, baton, handcuffs) • recognizing and handling "abnormal" persons • using the Incident Command System • report writing procedures • state uniform wear law	2-basic	3- working	4- advanced	1	2	3	4	5	6	7
15: Chemical, biological, radiological, nuclear, and explosive (CBRNE) and HAZMAT standards, requirements, and techniques including appropriate response protocols	1-limited	3- working	4- advanced	1	2	3	4	5	6	7
16: Conventional arms, ammunition, and explosives security standards, requirements, and techniques including, but not limited to: • principles for determining threat of arms, ammunition, and explosives • protection levels needed for specific weapons and ammunitions (including construction standards for building armory) • concept of sympathetic detonation and protection measures available for use	2-basic	3- working	4- advanced	1	2	3	4	5	6	

Occupational & Technical Knowledge & Skills	Complexity Level by Seniority			Relevant to CWFs						
	Entry	Journeyman	Senior							
17: Civil disturbance operations and emergency planning including, but not limited to: • principles for developing a resource plan and other aspects needed to provide emergency response • principles for developing and establishing emergency plans (including training as to what responses are appropriate) • principles for establishing security evacuation procedures (including related protections needed when outside the evacuated area) • principles for developing an internal emergency response plan • principles for coordinating with functional experts (e.g., fire department, medical, HAZMAT, outside agencies) to determine executability and applicability of existing bomb threat plans • principles for establishing procedures to reduce/minimize mass-casualty producing events	1- limited	3- working	4- advanced	1	2	3	4	5	6	7
19: Combating terrorism techniques including determining threat conditions, assessment of risks, and development of countermeasures	2-basic	4- advanced	5- expert	1	2	3	4	5	6	7
20: Principles for designing buildings and posts to address terrorist threat	2-basic	4- advanced	4- advanced	1	2	3	4	5	6	7
21: Design of exercises to test security force effectiveness	1- limited	4- advanced	4- advanced		2	3			6	
22: Laws and regulations governing the release of information (e.g., FOIA, Privacy Act)	2-basic	3- working	4- advanced	1	2	3	4	5	6	7
23: Information, personnel, technical, industrial, operations, and information systems security requirements as related to physical security	2-basic	4- advanced	4- advanced	1	2	3	4	5	6	7

Occupational & Technical Knowledge & Skills	Complexity Level by Seniority			Relevant to CWFs						
	Entry	Journeyman	Senior							
24: Engineering terminology and methods pertaining to construction, barriers, space ultilization, electrical schematics, and blueprints for facility and protective system design including, but not limited to: • using maps and geographical coordinate systems • relationship between construction materials/structures and security protection measures • reading blueprints and schematics • protective engineering designs and standards • applying internal control techniques, to include use of environmental and building design features • interpreting design and engineering documents	2-basic	4- advanced	4- advanced	1	2	3	4	5	6	7
25: Security investigation methods and techniques including, but not limited to: • methods for analyzing security incident trends and statistical data	1- limited	3- working	4- advanced	1	2	3	4	5	6	7
26: Contracting, procurement, acquisition and technical proposal evaluations related to physical security including, but not limited to: • elements of statements of work (SOW) • physical security impact of constraints from agreements • contract administration guidelines and principles • procedures for evaluating the physical security dimensions of MOUs and MOAs	1- limited	3-working	4- advanced	1	2	3	4	5	6	7

Occupational & Technical Knowledge & Skills	Complexity Level by Seniority			Relevant to CWFs						
	Entry	Journeyman	Senior							
27: Regulations governing the security of special security operations and/or areas including, but not limited to: • protective characteristics and functions of specialized shelter/bunker • requirements for use of vaults and containers • principles for coordinating movement of assets and associated levels of protections (including applicable guidelines and procedures) • principles for determining/analyzing how required courier/escort services will be executed	2-basic	4- advanced	4- advanced	1			4	5	6	
28: Property and supply accountability directives, regulations and procedures	2-basic	3- working	3- working	1						
29: Regulations and procedures related to controlled cryptographic gear and items	2-basic	3- working	4- advanced				4			
30: Protocols for evaluating, coordinating, and implementing physical security training and instruction including, but not limited to: • determining training needs, methodologies, and how to conduct appropriate training • principles for identifying individual skill sets, previous training, experience, and education to perform associated tasks • principles for identifying training agenda, scope, material, and how to determine outcomes	1- limited	3- working	4- advanced			3				7

Occupational & Technical Knowledge & Skills	Complexity Level by Seniority			Relevant to CWFs						
	Entry	Journeyman	Senior							
31: Physical security funding, manpower requirements, and budgeting programs including, but not limited to: • principles for determining manpower requirements • principles for analyzing costs and benefits associated with physical security options • principles for determining priority to meet identified requirements • principles for determining manpower utilization • principles for identifying available resources, how to obtain resources, and how to determine scope of resource needs based on mission and directives • financial management principles (e.g., budget management and control; cost and benefit analysis) • principles for conducting A-76 studies (e.g., comparing govt. and contract work) and how it relates to govt. jobs and costs	1- limited	3- working	5- expert	1	2	3	4	5	6	7
32: Federal, state, and local emergency management organizations and procedures including, but not limited to: • emergency services and how to determine physical security significance of service constraints • local agencies, their capabilities, and response characteristics • internal/external service capabilities • concurrent agreements • principles for establishing alert call list	2-basic	4- advanced	4- advanced	1	2	3	4	5	6	7
33: National fire prevention codes applicable to physical security including, but not limited to: • applying basic NFPA life safety standards and other code requirements relating to physical security • basic fire behavior principles	2-basic	3- working	4- advanced	1		3	4	5	6	
34: K9 concepts, procedures, and guidelines	1- limited	3- working	3- working						6	

APPENDIX I

SKILL STANDARDS FOR THE SECURITY INVESTIGATIONS DISCIPLINE

SKILL STANDARDS FOR THE SECURITY INVESTIGATIONS DISCIPLINE

OVERVIEW

This appendix contains skill standards for the Security Investigations discipline. It is important to understand skill standards terminology, abbreviations, and what the skill standards are before using this appendix. Appendix C, *Skill Standards Overview for Users of Appendices D-J*, describes the skill standards in detail. Carefully review Appendix C before using this appendix.

The content of this appendix consists of:

- Skill Standard I-1: Security Investigations Taxonomy
- Skill Standard I-2: Knowledge and Performance Levels Required on KAs in Relation to Seniority Level for Security Investigations
- Skill Standard I-3: A&E K&S Importance by Seniority and Relevant CWFs for Security Investigations
- Skill Standard I-4: Complexity Level by Seniority and Relevant CWFs for OTKS for Security Investigations

Skill Standard I-1
Security Investigations Taxonomy

CWF1: Initiate Investigation

- KA1: Determine Necessity of Investigation
  - Preliminary inquiry is conducted
  - Investigative jurisdiction and authority is confirmed
  - Type of investigation (criminal or administrative) is continually evaluated
- KA2: Determine Level of Classification, Compartmentation, and Sensitive Inhibiting Factors
  - Sensitive considerations that constrain the investigation are assessed
  - Access to and use of relevant data are verified
  - Who has security decision cognizance is determined
  - Sensitivity, security, and investigative equities are appropriately balanced
  - Coordination of matters of sensitivity, security, and compartmentation is determined
- KA3: Review Investigative Requirements
  - Scope of investigation is defined
  - Case file content is determined
  - Applicable investigative guidelines are evaluated
  - Investigative support resources are identified
  - Applicable investigative decision points are identified
  - Communication with other interested parties is established
- KA4: Review Predicatory Information
  - Relevant subject matter is defined
  - Laws, regulations, or procedures that may have been abridged are identified
  - Locations and persons of interest are identified
  - Jurisdictional authority over locations and persons is identified
  - Unresolved issues are identified
  - All jurisdictional considerations are addressed
- KA5: Develop Investigative Plan
  - Investigative objectives and requirements are defined
  - Investigative methodology is defined
  - Investigative resources are defined
  - Need for technical investigative support (i.e., photographic, fingerprint, polygraph, technical surveillance, forensic, and information technology technicians) is defined
  - Investigative activities are scheduled
  - Investigative plan is written and initiated

CWF2: Locate and Review Information

- KA6: Identify Individuals and Organizations of Investigative Interest
  - Necessary files, forms, and releases are reviewed
  - Subject matter issues and investigative leads are identified
- KA7: Review Incident Scene and Document Existing Conditions
  - Scene is preserved and protected
  - Potential hazards are considered
  - Witnesses and persons of interest are identified
  - Other locations of interest are identified
  - Relevant information are identified, collected, and documented
  - Need for incident scene photography is evaluated
  - Need for forensic technicians is evaluated
  - Need for information technology assistance is evaluated
- KA8: Identify and Review Other Sources of Information
  - Potential sources of recorded information are listed
  - Authority to collect information is obtained
  - Time-sensitive information are identified and preserved
  - Potential sources of unavailable information are identified

CWF3: Conduct Interviews

- KA9: Prepare for Interviews

  - Interviews are scoped based on requirements
  - Interview locations are determined
  - Safety and threat conditions are determined
  - Objectives are defined and interviews planned
  - Need for covert and overt investigative applications is determined
  - Response to request for witness or counsel is established
  - Confidentiality considerations are addressed
  - Authority and need to administer oath are determined
  - Investigative status of interviewees is determined
  - Applicable rights, warnings, waivers, and legal assurances are determined
  - Appropriate parties are notified
  - Interviews are scheduled
- KA10: Implement Interview Plan
  - Purpose of interview is explained
  - Procedures for documenting the interview are explained
  - Personal information is verified
  - Citizenship and status are determined
  - If necessary, oath is administered to facilitate formal statements
  - Questions are asked, responses are evaluated, and follow-ups conducted
  - Materials, evidence, and statements are collected
  - Interview is concluded and confidentiality rules explained

CWF4: Process Information

- KA11: Analyze Results
  - Information is evaluated
  - Status of investigative issues are determined
  - Unresolved issues are identified
  - Status of pursuit of reasonable sources and leads are determined
  - Remaining issues are addressed, as necessary

CWF5: Accomplish Other Investigative Activities

- KA12: Address Physical and Technical Surveillance Needs
  - Legal, regulatory, and procedural requirements are reviewed
  - Procedures and standards are applied
  - Surveillance needs are identified
  - Operational risk assessments are conducted
  - Surveillance is planned and executed
- KA13: Process Evidence
  - Legal, regulatory, and procedural requirements are reviewed
  - Procedures and standards are applied
  - Individuals with access to or collected evidence are identified and documented
  - Location where evidence was collected is identified
  - Evidence is properly documented
  - “Chain of custody” is documented
- KA14: Address Confidential Sources
  - Legal, regulatory, and procedural requirements are reviewed
  - Granting confidentiality is assessed
  - Procedures and standards are applied
  - Authority to grant confidentiality is secured
  - Confidentiality of source is protected
- KA15: Conduct Search and Seizure
  - Legal, regulatory, and procedural requirements are reviewed
  - Process to seal an area pending a search is determined
  - Execution of search is planned
  - Authority to seal an area or container pending a search is obtained
  - Authority to search and seize materials and evidence is obtained
  - Search is executed and evidence documented

- KA16: Manage Informants
    - Legal, regulatory, and procedural requirements are reviewed
    - Procedures and standards are applied
    - Informant’s motivation, reliability, and ability to provide relevant information are assessed
    - Information provided are evaluated
- KA17: Conduct Undercover Investigations
    - Legal, regulatory, and procedural requirements are reviewed
    - Procedures and standards are applied
    - Need for an undercover operation is determined
    - Protocols are identified and confirmed
    - Qualified and available operatives are identified
    - Operational risk assessment is conducted
    - Operational plan is developed

CWF6: Present Results of Investigation

- KA18: Produce Investigative Reports
    - Communication with interested parties is established
    - Investigator notes are safeguarded
    - Reports are prepared
- KA19: Present Testimony
    - Case is reviewed with legal counsel
    - Testimony and location are identified
    - Expert witness status is determined
    - Preparation for necessary depositions are made

Skill Standard I-2
Knowledge and Performance Levels Required on KAs in Relation to Seniority Level for Security Investigations

Key Activity	Knowledge Level by Seniority			Performance Level by Seniority		
	Entry	Journeyman	Senior	Entry	Journeyman	Senior
1. Determine Necessity of Investigation	B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	4-high	4-high
2. Determine Level of Classification, Compartmentation, and Sensitive Inhibiting Factors	A-nomenclature	B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	1-limited	2-partial	4-high
3. Review Investigative Requirements	B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	4-high	4-high
4. Review Predicatory Information	B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	4-high	4-high
5. Develop Investigative Plan	B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	4-high	4-high
6. Identify Individuals and Organizations of Investigative Interest	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
7. Review Incident Scene and Document Existing Conditions	B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	4-high	4-high
8. Identify and Review Other Sources of Information	B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	4-high	4-high
9. Prepare for Interviews	B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	4-high	4-high
10. Implement Interview Plan	B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	4-high	4-high
11. Analyze Results	B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	4-high	4-high
12. Address Physical and Technical Surveillance Needs	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high

APPENDIX I

Key Activity	Knowledge Level by Seniority			Performance Level by Seniority		
	Entry	Journeyman	Senior	Entry	Journeyman	Senior
13. Process Evidence	B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	4-high	4-high
14. Address Confidential Sources	B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	4-high	4-high
15. Conduct Search and Seizure	B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	4-high	4-high
16. Manage Informants	B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	4-high	4-high
17. Conduct Undercover Investigations	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
18. Produce Investigative Reports	B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	4-high	4-high
19. Present Testimony	B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	4-high	4-high

Skill Standard I-3
A&E K&S Importance by Seniority and Relevant CWFs for Security Investigations

Academic & Employability Knowledge & Skills	Importance by Seniority			Relevant CWFs					
	Entry	Journeyman	Senior	1	2	3	4	5	6
1. Ability to Learn—Recognize and use learning techniques and recall available information to apply and adapt new knowledge and skills in both familiar and changing situations. Use multiple approaches when learning new things. Assess how one is doing when learning or doing something. Keep up to date technically and know one's own job and related jobs.	●	●	●	1	2	3	4	5	6
2. Adaptability—Change one's own behavior or work methods to adjust to other people or to changing situations or work demands; be receptive to new information, ideas or strategies to achieve goals.	●	●	●	1	2	3	4	5	6
3. Analyzing and Solving Problems—Anticipate or identify problems and their causes; develop and analyze potential solutions or improvements using rational and logical processes or innovations and creative approaches when needed.	●	●	●	1	2	3	4	5	6
4. Building Consensus—Build consensus among individuals or groups by facilitating agreements that involve sharing or exchanging resources or resolving difference in such a way as to promote mutual goals and interest; by persuading others to change their points of view or behavior without losing their future support; and by resolving conflicts, confrontation, and disagreements while maintaining productive working relationships.	n/a	●	●	1	2	3	4	5	6
5. Gathering and Analyzing Information—Obtain facts, information or data relevant to a particular problem, question or idea through observation of events or situations, discussions with others, or research or retrieval from written or electronic sources; organize, integrate, analyze and evaluate information.	●	●	●	1	2	3	4	5	6
6. Initiative/Motivation—Exert a high level of effort and perseverance towards goal attainment. Work hard to become excellent at doing tasks by setting high standards, paying attention to details, working well and displaying a high level of concentration even when assigned an unpleasant task. Display high standards of attendance, punctuality, enthusiasm, vitality and optimism in approaching and completing tasks. Demonstrate willingness to take on responsibilities and challenges and do what is needed without being asked.	●	●	●	1	2	3	4	5	6
7. Integrity/Honesty—Demonstrate dependability, conscientiousness, integrity and accountability. Show commitment to doing the job carefully and correctly. Fulfill obligations and be reliable, responsible and trustworthy. Perform tasks thoroughly and completely. Demonstrate honesty and avoidance of unethical behavior.	●	●	●	1	2	3	4	5	6

Academic & Employability Knowledge & Skills	Importance by Seniority			Relevant CWFs					
	Entry	Journeyman	Senior	1	2	3	4	5	6
8. Leading Others—Motivate, inspire, and influence others toward effective individual or teamwork performance, goal attainment, and personal learning and development by serving as a mentor, coach and role model and by providing feedback and recognition or rewards.	n/a	●	●	1	2	3	4	5	6
9. Listening—Attend to, receive and correctly interpret verbal communications and directions through cues such as the content and context of the message and the tone, gesture and facial expression of the speaker.	●	●	●	1	2	3	4	5	6
10. Maintain Professional Demeanor—Demonstrate credibility and authority in issuing instructions and making requests to individuals and in performing duties. Maintains firm and direct tone of voice, authoritative posture, manner and bearing.	n/a	●	●	1	2	3	4	5	6
11. Making Decisions and Judgments—Make decisions that consider relevant facts and information, potential risks and benefits, and short- and long-term consequences or alternatives.	●	●	●	1	2	3	4	5	6
12. Mathematics—Understand, interpret and manipulate numeric or symbolic information; solve problems by selecting and applying appropriate quantitative methods such as arithmetic and estimation.	n/a	●	●	1	2	3	4	5	6
13. Organizing and Planning—Organize and structure work for effective performance and goal attainment; set and balance priorities; anticipate obstacles; formulate plans consistent with available human, financial, and physical resources; modify plans or adjust priorities given changing goals or conditions.	n/a	●	●	1	2	3	4	5	6
14. Reading—Understand and use written information that may be presented in a variety of formats, such as text, tables, lists, figures, and diagrams; select reading strategies appropriate to the purpose, such as skimming for highlights, reading for detail, reading for meaning and critical analysis.	●	●	●	1	2	3	4	5	6
15. Science—Understand and apply the basic principles of physical, chemical, biological and earth sciences, understand and apply the scientific method, including formulating and stating hypotheses and evaluating them by experimentation or observation.	n/a	●	●	1	2	3	4	5	6
16. Self and Career Development—Identify own work and career interests, strengths and limitations; pursue education, training, feedback or other opportunities for learning and development; manage, direct and monitor one's own learning and development.	●	●	●	1	2	3	4	5	6
17. Speaking—Express ideas and facts orally in a clear and understandable manner that sustains listener attention and interest; tailor oral communications to the intended purpose and audience.	●	●	●	1	2	3	4	5	6

Academic & Employability Knowledge & Skills	Importance by Seniority			Relevant CWFs					
	Entry	Journeyman	Senior	1	2	3	4	5	6
18. Stress Tolerance—Demonstrate maturity, poise and restraint to cope with pressure, stress, criticism, setbacks, personal and work-related problems, etc. Maintain composure, keeping emotions in check, controlling anger, and avoiding aggressive behavior even in very difficult situations. Accept criticism and deal calmly and effectively with high-stress situations.	●	●	●	1	2	3	4	5	6
19. Using Information and Communications Technology—Select, access and use necessary information, data, and communications-related technologies, such as basic personal computer applications, telecommunications equipment, Internet, electronic calculators, voice mail, email, facsimile machines and copying equipment to accomplish work activities.	●	●	●	1	2	3	4	5	6
20. Using Interpersonal Skills—Interact with others in ways that are friendly, courteous and tactful and that demonstrate respect for individual and cultural differences and for the attitudes and feelings of others.	●	●	●	1	2	3	4	5	6
21. Visual Observation—Notice details and take in and recall incoming visual sensory information and use it to make predictions, comparisons and/or evaluations. Recognize differences or similarities, or sensing changes in circumstances or events; discern between relevant visual cues or information and irrelevant or distracting information.	●	●	●	1	2	3	4	5	6
22. Working in Teams—Work cooperatively and collaboratively with others to achieve goals by sharing or integrating ideas, knowledge, skills, information, support, resources, responsibility and recognition.	●	●	●	1	2	3	4	5	6
23. Writing—Express ideas and information in written form clearly, succinctly, accurately, and in an organized manner; use English language conventions or spelling, punctuation, grammar, and sentence and paragraph structure; and tailor written communication to the intended purpose and audience.	●	●	●	1	2	3	4	5	6

Skill Standard I-4
Complexity Level by Seniority and Relevant CWFs for OTKS for Security Investigations

Occupational & Technical Knowledge & Skills	Complexity Level by Seniority			Relevant to CWFs					
	Entry	Journeyman	Senior						
1. Laws, policies, regulations, and guidelines applicable to the conduct of investigations	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4	5	6
2. Nature, types, and categories of ethical issues related to cases (including, but not limited to): • Fiduciary • Conflict of interest • Attorney-client • Applicable aspects of laws, codes, and regulations	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4	5	6
3. Investigation concepts, principles, and practices (including, but not limited to): • Types of investigations: Administrative vs. Criminal • Scope of investigations • Coverage requirements for each type of investigation	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4	5	6
4. Case and time management strategies	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4	5	6
5. Interviewing and interrogation techniques (including, but not limited to): • Policies regarding interviews and recording of interviews • Handling requests for presence of representation during interviews • Techniques for detecting deception • Methods and techniques of eliciting admission and/or confession	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4	5	6
6. Guidance regarding proper taking, use and handling of investigative notes	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4	5	6
7. Concepts, principles, and practices of polygraph use	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4	5	6
8. Case-related information regarding government and private organizations' functions and structure	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4	5	6

Occupational & Technical Knowledge & Skills	Complexity Level by Seniority			Relevant to CWFs					
	Entry	Journeyman	Senior						
9. Concepts, principles, and practices associated with standard reporting format	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4	5	6
10. Agency-specific terminology, structure, instructions, correspondence procedures, or regulations	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4	5	6
11. Terminologies (including, but not limited to): • Medical/mental health terminology • Financial terminology • Legal terminology • Alcohol/Drug terminology • Criminal behavior terminology • Immigration and naturalization terminology	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4	5	6
12. Unique/precedent-setting case laws	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4	5	6
13. Computer and information systems usage guidelines	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4	5	6
14. Hostile countries and organizations	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4	5	6
15. Concepts and principles of clearance, access, reliability, suitability, and trustworthiness	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4	5	6
16. IT-based applications related to investigation (proper use, rules and guidelines)	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4	5	6
17. Concepts, principles, and practices of proper control of records	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4	5	6
18. Third party release provisions	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4	5	6
19. Record management requirements as related to investigations	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4	5	6

Occupational & Technical Knowledge & Skills	Complexity Level by Seniority			Relevant to CWFs					
	Entry	Journeyman	Senior						
20. Vital records concepts, principles, and practices	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4	5	6
21. Civil and Criminal Laws (including, but not limited to): • Judicial Precedents • Rights of Suspects • Arrest Procedures • Criminal Procedures	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4	5	6
22. Rules of Evidence (including, but not limited to): • Chain-of-custody procedures and requirements • Methods and procedures for preserving various types of evidence • Forensic concepts and procedures	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4	5	6
23. Surveillance Principles, Practices, and Methods	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4	5	6
24. Inspection and detection techniques	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4	5	6
25. Physical, Information, Information Systems, Personnel, Communications Security Concepts	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4	5	6
26. Document Review Techniques	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4	5	6
27. Health and Safety Concepts and Principles	2-basic	4-advanced 3-working	5-expert 4-advanced	1	2	3	4	5	6

APPENDIX J

SKILL STANDARDS FOR THE SECURITY MANAGEMENT DISCIPLINE

SKILL STANDARDS FOR THE SECURITY MANAGEMENT DISCIPLINE

OVERVIEW

This appendix contains skill standards for the Security Management discipline. It is important to understand skill standards terminology, abbreviations, and what the skill standards are before using this appendix. Appendix C, *Skill Standards Overview for Users of Appendices D-J*, describes the skill standards in detail. Carefully review Appendix C before using this appendix.

The content of this appendix consists of:

- Subject-Matter Expert Notes
- Skill Standard J-1: Security Management Taxonomy
- Skill Standard J-2: Knowledge and Performance Levels Required on KAs in Relation to Seniority Level for Security Management
- Skill Standard J-3: A&E K&S Importance by Seniority and Relevant CWFs for Security Management
- Skill Standard J-4: Complexity Level by Seniority and Relevant CWFs for OTKS for Security Management

SUBJECT-MATTER EXPERT NOTES

SMEs who contributed to the development of Security Management skill standards observed that performing the Security Management function depends on a security manager's scope of responsibility in terms of various security disciplines, such as personnel security, physical security, information security, information systems security, security investigations, or communications security. Different security managers may share the same job title but do quite different work.

APPENDIX J

Skill Standard J-1
Security Management Taxonomy

CWF1: Determine Security Program Needs

- KA1: Document Mission Needs
  - Mission objectives are identified
  - Critical capabilities and assets are determined
  - Operational imperatives are established
  - Protection applications are developed
- KA2: Identify Duties to Protect
  - Duties imposed by laws and regulations are confirmed
  - Duties set by agreement and contract are researched
  - Self-imposed duties are evaluated
  - Additional protection duties are determined
  - Asset criticality analysis is performed
- KA3: Identify Scope of Possible Security Requirements
  - Physical security requirements are evaluated
  - Personnel security requirements are evaluated
  - Information security requirements are evaluated
  - Information systems security requirements are evaluated
  - Information assurance requirements are evaluated
  - Communications security requirements are evaluated
  - Investigations requirements are evaluated
  - Intelligence and counterintelligence requirements are evaluated
  - Technical means requirements are evaluated
  - Compartmentation requirements are evaluated
  - Operations security requirements are evaluated
  - Industrial security requirements are evaluated
- KA4: Conduct Risk Determination Process
  - Mission loss impact is determined
  - Threat analysis is conducted
  - Vulnerability analysis is conducted
  - Countermeasures are determined
- KA5: Determine Emergency Services
  - Disaster plans are developed
  - Fire, medical, and police responses are coordinated
  - Workplace safety and violence prevention are reviewed
  - Continuity of Operations (COOP) are addressed

CWF2: Implement Security Programs

- KA6: Develop Security Plan
  - Security measures are selected
  - Operational integration is considered
  - Operational impact is reviewed
  - Emergency planning is coordinated
  - Legal implications are considered
  - Security policies are reviewed
  - Approval is obtained
  - Plan is implemented and validated
  - Strategic planning processes are applied
- KA7: Develop Workforce Knowledge and Skills
  - Requirements are determined
  - Technical capabilities of workforce are developed
  - Management capabilities of workforce are developed
  - Leadership capabilities of workforce are developed
  - Ethical behavior is assured
- KA8: Allocate Resources

    - Resources are identified
    - Sources and costs are determined
    - Return-on-investment is calculated
    - Approval(s) are obtained

CWF3: Manage Ongoing Program

- KA9: Establish Program Measurements
    - Accountability standards are defined
    - Element auditing is conducted
    - Testing of program objectives is performed
    - Surveys are conducted
    - Results are analyzed
- KA10: Monitor Needs and Changes
    - Mission objectives are evaluated
    - Threats and vulnerabilities are reviewed
    - Validity of security measures is established
    - Impact of technological changes is evaluated
    - Impact of policy changes is evaluated
    - Program ethics and integrity are evaluated
- KA11: Implement Program Modifications
    - Mission needs are reviewed
    - Resource plan(s) are reviewed
    - Security plan is modified
- KA12: Create Budget for Program Security Measures
    - Mission resource requirements are determined
    - Funding mechanisms are determined
    - Reprogramming is accomplished
- KA13: Apply Information Processing Technologies
    - System(s) Architecture is designed
    - Constraints are determined
    - Automatic monitoring is implemented
    - Changes in technology system(s) are addressed
- KA14: Determine education, training, and awareness needs
    - Requirements are identified
    - Needs are determined
    - Training is developed and implemented
    - Needs are continuously evaluated
    - Training effectiveness are continuously evaluated

Skill Standard J-2
Knowledge and Performance Levels Required on KAs in Relation to Seniority Level for Security Management

Key Activity	Knowledge Level by Seniority			Performance Level by Seniority		
	Entry	Journeyman	Senior	Entry	Journeyman	Senior
1. Document mission needs	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
2. Identify duties to protect	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
3. Identify scope of possible security requirements	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	2-partial	3-competent	3-competent
4. Conduct risk determination process	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
5. Determine emergency services	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
6. Develop security plan	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
7. Develop workforce knowledge and skills	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
8. Allocate resources	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
9. Establish program measurements	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	2-partial	3-competent	3-competent
10. Monitor needs and changes	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
11. Implement program modifications	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high
12. Create budget for program security measures	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	3-competent

Key Activity	Knowledge Level by Seniority			Performance Level by Seniority		
	Entry	Journeyman	Senior	Entry	Journeyman	Senior
13. Apply information processing technologies	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	2-partial	3-competent	3-competent
14. Determine education, training, and awareness needs	B-procedures A-nomenclature	C-principles B-procedures A-nomenclature	D-theory C-principles B-procedures A-nomenclature	2-partial	3-competent	4-high

Skill Standard J-3
A&E K&S Importance by Seniority and Relevant CWFs for Security Management

Academic & Employability Knowledge & Skills	Importance by Seniority			Relevant CWFs		
	Entry	Journeyman	Senior	1	2	3
1. Ability to Learn—Recognize and use learning techniques and recall available information to apply and adapt new knowledge and skills in both familiar and changing situations. Use multiple approaches when learning new things. Assess how one is doing when learning or doing something. Keep up to date technically and know one's own job and related jobs.	●	●	●	1	2	3
2. Adaptability—Change one's own behavior or work methods to adjust to other people or to changing situations or work demands; be receptive to new information, ideas or strategies to achieve goals.	●	●	●	1	2	3
3. Analyzing and Solving Problems—Anticipate or identify problems and their causes; develop and analyze potential solutions or improvements using rational and logical processes or innovations and creative approaches when needed.	●	●	●	1	2	3
4. Building Consensus—Build consensus among individuals or groups by facilitating agreements that involve sharing or exchanging resources or resolving difference in such a way as to promote mutual goals and interest; by persuading others to change their points of view or behavior without losing their future support; and by resolving conflicts, confrontation, and disagreements while maintaining productive working relationships.	●	●	●	1	2	3
5. Gathering and Analyzing Information—Obtain facts, information or data relevant to a particular problem, question or idea through observation of events or situations, discussions with others, or research or retrieval from written or electronic sources; organize, integrate, analyze and evaluate information.	●	●	●	1	2	3
6. Initiative/Motivation—Exert a high level of effort and perseverance towards goal attainment. Work hard to become excellent at doing tasks by setting high standards, paying attention to details, working well and displaying a high level of concentration even when assigned an unpleasant task. Display high standards of attendance, punctuality, enthusiasm, vitality and optimism in approaching and completing tasks. Demonstrate willingness to take on responsibilities and challenges and do what is needed without being asked.	●	●	●	1	2	3
7. Integrity/Honesty—Demonstrate dependability, conscientiousness, integrity and accountability. Show commitment to doing the job carefully and correctly. Fulfill obligations and be reliable, responsible and trustworthy. Perform tasks thoroughly and completely. Demonstrate honesty and avoidance of unethical behavior.	●	●	●	1	2	3
8. Leading Others—Motivate, inspire, and influence others toward effective individual or teamwork performance, goal attainment, and personal learning and development by serving as a mentor, coach and role model and by providing feedback and recognition or rewards.	●	●	●	1	2	3
9. Listening—Attend to, receive and correctly interpret verbal communications and directions through cues such as the content and context of the message and the tone, gesture and facial expression of the speaker.	●	●	●	1	2	3
10. Maintain Professional Demeanor—Demonstrate credibility and authority in issuing instructions and making requests to individuals and in performing duties. Maintains firm and direct tone of voice, authoritative posture, manner and bearing.	●	●	●	1	2	3
11. Making Decisions and Judgments—Make decisions that consider relevant facts and information, potential risks and benefits, and short- and long-term consequences or alternatives.	●	●	●	1	2	3
12. Mathematics—Understand, interpret and manipulate numeric or symbolic information; solve problems by selecting and applying appropriate quantitative methods such as arithmetic and estimation.	●	●	●	1	2	3
13. Organizing and Planning—Organize and structure work for effective performance and goal attainment; set and balance priorities; anticipate obstacles; formulate plans consistent with available human, financial, and physical resources; modify plans or adjust priorities given changing goals or conditions.	●	●	●	1	2	3

Academic & Employability Knowledge & Skills	Importance by Seniority			Relevant CWFs		
	Entry	Journeyman	Senior	1	2	3
14. Reading—Understand and use written information that may be presented in a variety of formats, such as text, tables, lists, figures, and diagrams; select reading strategies appropriate to the purpose, such as skimming for highlights, reading for detail, reading for meaning and critical analysis.	●	●	●	1	2	3
15. Science—Understand and apply the basic principles of physical, chemical, biological and earth sciences, understand and apply the scientific method, including formulating and stating hypotheses and evaluating them by experimentation or observation.	n/a	n/a	n/a			
16. Self and Career Development—Identify own work and career interests, strengths and limitations; pursue education, training, feedback or other opportunities for learning and development; manage, direct and monitor one's own learning and development.	●	●	●	1	2	3
17. Speaking—Express ideas and facts orally in a clear and understandable manner that sustains listener attention and interest; tailor oral communications to the intended purpose and audience.	●	●	●	1	2	3
18. Stress Tolerance—Demonstrate maturity, poise and restraint to cope with pressure, stress, criticism, setbacks, personal and work-related problems, etc. Maintain composure, keeping emotions in check, controlling anger, and avoiding aggressive behavior even in very difficult situations. Accept criticism and deal calmly and effectively with high-stress situations.	●	●	●	1	2	3
19. Using Information and Communications Technology—Select, access and use necessary information, data, and communications-related technologies, such as basic personal computer applications, telecommunications equipment, Internet, electronic calculators, voice mail, email, facsimile machines and copying equipment to accomplish work activities.	●	●	●	1	2	3
20. Using Interpersonal Skills—Interact with others in ways that are friendly, courteous and tactful and that demonstrate respect for individual and cultural differences and for the attitudes and feelings of others.	●	●	●	1	2	3
21. Visual Observation—Notice details and take in and recall incoming visual sensory information and use it to make predictions, comparisons and/or evaluations. Recognize differences or similarities, or sensing changes in circumstances or events; discern between relevant visual cues or information and irrelevant or distracting information.	●	●	●	1	2	3
22. Working in Teams—Work cooperatively and collaboratively with others to achieve goals by sharing or integrating ideas, knowledge, skills, information, support, resources, responsibility and recognition.	●	●	●	1	2	3
23. Writing—Express ideas and information in written form clearly, succinctly, accurately, and in an organized manner; use English language conventions or spelling, punctuation, grammar, and sentence and paragraph structure; and tailor written communication to the intended purpose and audience.	●	●	●	1	2	3

Skill Standard J-4
Security Disciplines and OTKS for Security Management

Notes:

The OTKS required to perform the Security Management function will depend on a security manager's scope of responsibility – the extent to which they are responsible for managing various security disciplines (i.e., personnel security, physical security, information security, information systems security, investigations, communications security).

It is expected that security managers will, at the very least, have "advanced knowledge" of the OTKS for the specific security disciplines they are responsible for. In other words, a security manager is expected to be able to:

- independently apply discipline-relevant knowledge or skills in moderately complex, difficult, or stressful situations or situations with moderately high consequences for error, and
- assist others in the application of the discipline-relevant knowledge or skill.

In addition, it is expected that security managers will, at the very least, have a "general familiarity or awareness of the concepts, principles, and fundamentals" of the OTKS for the security disciplines they are not responsible for.

The specific OTKS relevant to each of the security discipline, delineated previously, are provided below.

Security Discipline	Occupational & Technical Knowledge & Skills
Personnel Security	1. Policies, regulations, guidelines and ethical standards that govern the conduct of Personnel Security Investigations (including, but not limited to): • Investigative standards • Section 1001 and 1905, Title XVIII US Code and other applicable laws • DCID 6/4 • EO 12968 • EO 10450 • Privacy Act 1974 & Freedom of Information Act • Ethical standards (prohibitions and forbidden topics) • Other policies and directives
	2. Adjudicative guidelines • Allegiance to the United States • Foreign influence • Foreign preference • Sexual Behavior • Personal Conduct • Financial considerations • Alcohol consumption • Drug involvement • Emotional, mental, personality disorders • Criminal conduct • Security violations • Outside activities • Misuse of information technology systems
	3. Investigation concepts, principles, and practices (including, but not limited to): • Types of investigations • Scope of investigations • Coverage requirements for each type of investigation (e.g., Single Scope Background Investigations (SSBI) and SSBI-Periodic Reinvestigations)
	4. Case and time management strategies
	5. Interviewing techniques (including, but not limited to): • Policies regarding telephonic interviews • Handling requests for presence of representation during interviews
	6. Guidance regarding proper taking, use and handling of investigative notes
	7. Threat situation and their impact (including, but not limited to): • counter-intelligence and counter-terrorism • personal safety and environment
	8. Concepts, principles, and practices of polygraph use
	9. Case-related information regarding government and private organizations' functions and structure
	10. Concepts, principles, and practices associated with standard reporting format
	11. Types of sources
	12. Concepts, principles, and practices associated with the application of adjudicative criteria, disqualifying factors, and mitigating factors
	13. Agency-specific terminology, structure, instructions, correspondence procedures, or regulations
	14. Levels of clearance and access
	15. Interim access criteria and justifications

Security Discipline	Occupational & Technical Knowledge & Skills
	16. Terminologies (including, but not limited to): • Medical/mental health terminology • Financial terminology • Legal terminology • Alcohol/Drug terminology • Criminal behavior terminology • Immigration and naturalization terminology
	17. Special Program case procedures (including, but not limited to): Special Access programs
	18. Physical security requirements associated with personnel security
	19. Computer and information systems usage guidelines (including, but not limited to): • IT-based applications related to personnel security (proper use, rules and guidelines)
	20. Concepts, principles, and practices of financial analysis
	21. Hostile countries and organizations
	22. Case processing procedures
	23. Information elicitation techniques
	24. Concepts and principles of clearance, access, reliability, suitability, and trustworthiness
	25. Computer and information systems usage guidelines (including, but not limited to): • IT-based applications related to personnel security (proper use, rules and guidelines)
	26. Concepts, principles, and practices of financial analysis
	27. Hostile countries and organizations
	28. Case processing procedures
	29. Information elicitation techniques
	30. Concepts and principles of clearance, access, reliability, suitability, and trustworthiness
	31. Ethical issues associated with personnel security
	32. Concepts, principles, and practices of proper control of records
	33. Third party release provisions
	34. Risk management concepts, principles, and practices
	35. Record management requirements as related to personnel security
	36. Information Assurance requirements as related to personnel security
	37. Information System Security requirements as related to personnel security
	38. Operations Security Program requirements as related to personnel security
	39. Personnel security-related funding, manpower requirements, and budgeting programs
	40. Communications Security Program requirements as related to personnel security
	41. Personnel security regulations and processes including protected information status, determination, assessment procedures, security, marking, control, accountability, and safeguarding of records
	42. Preparation, coordination, and execution of MOU, MOA, Interservice Support Agreements, and Service Level Agreements
	43. Program evaluation concepts, methods, and techniques
	44. National disclosure policies
	45. Development, preparation, and execution of personnel security presentations and briefings
	46. Development, preparation, and execution of personnel security plans
	47. Development, preparation, and execution of personnel security policies and procedures
	48. Vital records concepts, principles, and practices
	49. Design and development of personnel security training and instruction
	50. Methods for analyzing, organizing, compiling, and reporting personnel security data

Security Discipline	Occupational & Technical Knowledge & Skills
Physical Security	51. Laws, regulations, concepts, principles, and technology related to physical security including, but not limited to: ● Interpretation of legal documents ● research processes and procedures ● principles for determining physical security measures to support mission ● principles for integrating physical security protocols to ensure appropriate level of protection ● deviation, waiver, and/or exception concept ● establishing location boundaries ● concept of Continuity of Government (COG) oversight ● Concept of operations (CONOP) for the specific site and/or mission regarding protective forces needed for operational personnel
	52. Developments and advances in security systems, methods, equipment, and techniques including, but not limited to: ● security equipments, operations, and sources of options ● evaluation of commercially available integrated systems ● principles for establishing technical standards (e.g., STC-TEMPEST) ● principles for defining technical security measures (e.g., IDS, CCTV, Guard Access Control) ● concept of protection levels ● technology types, levels and applications ● C3I requirements (e.g., elements of facility construction and limitations, types of systems/equipment required) ● development of plans and procedures to operate physical security-related systems ● procedures for establishing a “3 level” (i.e., telephone, radio, RF) communication system ● principles for establishing training and maintenance requirements to manage security system sustainability
	53. Physical security regulations and procedures required to protect mission essential areas including, but not limited to: ● principles for establishing operations/mission of special security areas ● unique operational requirements of special security areas ● principles for establishing inspection and certification processes associated with special security areas
	54. Interview and elicitation techniques
	55. Physical security survey/inspection and technical site survey inspection techniques including, but not limited to: ● physical security regulations for initiating inspections, assessments, and/or reviews ● concepts, principles, and methods for determining effectiveness of security measures, operability, and performance testing ● use and interpretation of analytical and software system data to evaluate and model facility security system

Security Discipline	Occupational & Technical Knowledge & Skills
	56. Multi-layered security systems involving access controls, barriers, protection devices, monitoring equipment, security forces, and intrusion detection equipment including, but not limited to: ● barrier types, their protective capabilities, and security effectiveness ● types of lighting, protective levels relative to lumens available, and power sources ● concepts and principles of time and distance factors (i.e., deny, delay) ● layered defense concept ● procedures for employing/deploying IDS/surveillance equipment to facilitate detection and response based on layered defense concept ● equipment, processes, and physical security measures to control access (technology integration) ● authorized access to specific areas versus general access ● use of monitoring and detection systems (e.g., IDS and CCTV)
	57. Methods for effective presentation of physical security and law enforcement data.
	58. Risk analysis and vulnerability assessment techniques including, but not limited to: ● principles and methods for assessing vulnerabilities ● principles and methods for identifying and verifying physical security threats ● principles and methods for assessing threats against physical security vulnerabilities ● principles and methods for evaluating threat and intelligence information
	59. Concepts, practices, and principles associated with recovery/restoration programs
	60. Development, preparation, and execution of physical security policies and procedures
	61. Concepts, principles, and practices related to crime prevention including, but not limited to: ● crime prevention, property, and inventory control and how to develop security plans associated with them ● methods for analyzing crime trends and statistical data
	62. Development, preparation, and execution of physical security plans including, but not limited to: ● operational impacts on physical security measures (e.g., sizing security areas against operational parameters and physical security requirements) ● relationship between the logistical, operational, and mission-driven requirements of location and security protection measures ● principles for developing and implementing response plans ● COOP plans to specifically include capabilities and respective limitations ● principles of how to determine level of command, control, communications, computer, and intelligence based on operational goals and objectives ● program evaluation principles (e.g., collect data, define physical security parameters, acknowledge problems, advise corrections, and evaluate programs) ● installation mobilization/deployment contingency plans, regulations, and procedures

Security Discipline	Occupational & Technical Knowledge & Skills
	63. Laws, regulations, concepts, principles, practices, and technology related to law enforcement operations including, but not limited to: ● local, state, federal legal requirements and standards (including their implications on authority and jurisdictional limitations) ● arrest powers and areas of cognizance ● law and policies relative to arrest, detention, search, inspection, and use of force ● local restrictions ● laws and techniques of search, seizure, and the use of force ● civil rights of individuals and the rights of suspects ● laws, regulations, and procedures pertaining to the collection, preservation, and accountability of evidence ● security concepts and procedures for vehicle movements and parking (e.g., traffic flow patterns, traffic control devices)
	64. Laws, regulations, concepts, principles, practices, and technology related to security guard operations including, but not limited to: ● principles associated with determining fixed posts and roving patrol needs, deployment, and response techniques, tactics and strategies ● writing post and patrol orders ● principles associated with determining and using individual and team guard force equipment ● applying First Aid and CPR ● using assigned weapons and intermediate force equipment (e.g., chemical, baton, handcuffs) ● recognizing and handling “abnormal” persons ● using the Incident Command System ● report writing procedures ● state uniform wear law
	65. Chemical, biological, radiological, nuclear, and explosive (CBRNE) and HAZMAT standards, requirements, and techniques including appropriate response protocols
	66. Conventional arms, ammunition, and explosives security standards, requirements, and techniques including, but not limited to: ● principles for determining threat of arms, ammunition, and explosives ● protection levels needed for specific weapons and ammunitions (including construction standards for building armory) ● concept of sympathetic detonation and protection measures available for use

Security Discipline	Occupational & Technical Knowledge & Skills
	67. Civil disturbance operations and emergency planning including, but not limited to: • principles for developing a resource plan and other aspects needed to provide emergency response • principles for developing and establishing emergency plans (including training as to what responses are appropriate) • principles for establishing security evacuation procedures (including related protections needed when outside the evacuated area) • principles for developing an internal emergency response plan • principles for coordinating with functional experts (e.g., fire department, medical, HAZMAT, outside agencies) to determine executability and applicability of existing bomb threat plans • principles for establishing procedures to reduce/minimize mass-casualty producing events
	68. Combating terrorism techniques including determining threat conditions, assessment of risks, and development of countermeasures
	69. Principles for designing buildings and posts to address terrorist threat
	70. Design of exercises to test security force effectiveness
	71. Laws and regulations governing the release of information (e.g., FOIA, Privacy Act)
	72. Information, personnel, technical, industrial, operations, and information systems security requirements as related to physical security
	73. Engineering terminology and methods pertaining to construction, barriers, space ultilization, electrical schematics, and blueprints for facility and protective system design including, but not limited to: • using maps and geographical coordinate systems • relationship between construction materials/structures and security protection measures • reading blueprints and schematics • protective engineering designs and standards • applying internal control techniques, to include use of environmental and building design features • interpreting design and engineering documents
	74. Security investigation methods and techniques including, but not limited to: • methods for analyzing security incident trends and statistical data
	75. Contracting, procurement, acquisition and technical proposal evaluations related to physical security including, but not limited to: • elements of statements of work (SOW) • physical security impact of constraints from agreements • contract administration guidelines and principles • procedures for evaluating the physical security dimensions of MOUs and MOAs
	76. Regulations governing the security of special security operations and/or areas including, but not limited to: • protective characteristics and functions of specialized shelter/bunker • requirements for use of vaults and containers • principles for coordinating movement of assets and associated levels of protections (including applicable guidelines and procedures) • principles for determining/analyzing how required courier/escort services will be executed
	77. Property and supply accountability directives, regulations and procedures

Security Discipline	Occupational & Technical Knowledge & Skills
	78. Regulations and procedures related to controlled cryptographic gear and items
	79. Protocols for evaluating, coordinating, and implementing physical security training and instruction including, but not limited to: ● determining training needs, methodologies, and how to conduct appropriate training ● principles for identifying individual skill sets, previous training, experience, and education to perform associated tasks ● principles for identifying training agenda, scope, material, and how to determine outcomes
	80. Physical security funding, manpower requirements, and budgeting programs including, but not limited to: ● principles for determining manpower requirements ● principles for analyzing costs and benefits associated with physical security options ● principles for determining priority to meet identified requirements ● principles for determining manpower utilization ● principles for identifying available resources, how to obtain resources, and how to determine scope of resource needs based on mission and directives ● financial management principles (e.g., budget management and control; cost and benefit analysis) ● principles for conducting A-76 studies (e.g., comparing govt. and contract work) and how it relates to govt. jobs and costs
	81. Federal, state, and local emergency management organizations and procedures including, but not limited to: ● emergency services and how to determine physical security significance of service constraints ● local agencies, their capabilities, and response characteristics ● internal/external service capabilities ● concurrent agreements ● principles for establishing alert call list
	82. National fire prevention codes applicable to physical security including, but not limited to: ● applying basic NFPA life safety standards and other code requirements relating to physical security ● basic fire behavior principles
	83. K9 concepts, procedures, and guidelines
Information Security	84. Information security regulations and processes including classification status determination, assessment procedures, security, classification, declassification, reclassification, marking, control, accountability, and safeguarding of records
	85. Developments and advances in information security systems, methods, equipment, and techniques
	86. Methods for analyzing, organizing, compiling, and reporting information security data
	87. Threat, vulnerability, and risk assessment techniques associated with information security
	88. Concepts, practices, and principles associated with recovery/restoration of information security program data
	89. Development, preparation, and execution of information security plans
	90. Development, preparation, and execution of information security policies and procedures
	91. Concepts, principles, and practices related to protected information loss prevention as it relates to information security
	92. Development, preparation, and execution of emergency and/or continuity plans as it related to information security

Security Discipline	Occupational & Technical Knowledge & Skills
	93. Laws and regulations governing the release of information (e.g., FOIA, Privacy Act), and Statutes and Executive Orders governing the protection of specific types of records (e.g., EO 12958 as amended, Atomic Energy Act, Section 119, Title X, U.S. Code). This includes (but is not limited to): ● regulations, concepts, and principles related to data aggregation ● security assistance policies including laws, regulations, and policies controlling U.S. transfer of arms and services to foreign governments and international organizations (e.g., Arms Export Control Act of 1976)
	94. Physical security requirements as related to information security
	95. Record management requirements as related to information security
	96. Information System Security requirements as related to information security
	97. Personnel Security Program requirements as related to information security
	98 . Operations Security Program requirements as related to information security
	99. Contracting, procurement, acquisition, research, and technical proposal evaluations related to information security (including content and format of technical contract specifications)
	100. Design and development of information security training and instruction
	101. Information security-related funding, manpower requirements, and budgeting programs
	102. Communications Security Program requirements as related to information security
	103. Information security regulations and processes including protected information status, determination, assessment procedures, security, marking, control, accountability, and safeguarding of records
	104. Development, preparation, and execution of information protection program (including the development, preparation, and application of protected information guidelines)
	105. Development, preparation, and execution of protected information handling procedures
	106. Program evaluation concepts, methods, and techniques
	107. Preparation, coordination, and execution of MOU, MOA, Interservice Support Agreements, and Service Level Agreements
	108. Protection concepts associated with the information assurance features of availability, integrity, authentication, confidentiality, and non-repudiation
	109. Integration of information technologies (e.g., biometrics, information tracking, bar code, geo-spatial information)
	110. Principles, concepts, and methods for information storage, distribution, and transportation
	111. Developments and advances in emerging technologies (e.g., PDAs, PEDs, wireless networks, internet/intranet, nanotechnology, and artificial intelligence) and their applications and trends in information management
	112. Media and equipment transportation policies including USPS regulations and transportation requirements for non-postal service carriers (e.g., government and federal courier agencies)
	113. Electronic, optical, and other energy transfer of information (e.g., laser, fax, email, and web pages) policies and requirements
	114. Classification management and other protected information concepts and terms (including concepts and principles of original and derivative classification)
	115. Equity recognition, decision support, and appeals
	116. Redaction techniques and processes
	117. National disclosure policies
	118. Protection principles associated with human knowledge
	119. Failure analysis concepts, methods, principles, and techniques
	120. Development, preparation, and execution of information security presentations and briefings
Security Investigations	121. Laws, policies, regulations, and guidelines applicable to the conduct of investigations

Security Discipline	Occupational & Technical Knowledge & Skills
	122. Nature, types, and categories of ethical issues related to cases (including, but not limited to): • Fiduciary • Conflict of interest • Attorney-client • Applicable aspects of laws, codes, and regulations
	123. Investigation concepts, principles, and practices (including, but not limited to): • Types of investigations: Administrative vs. Criminal • Scope of investigations • Coverage requirements for each type of investigation
	124. Interviewing and interrogation techniques (including, but not limited to): • Policies regarding interviews and recording of interviews • Handling requests for presence of representation during interviews • Techniques for detecting deception • Methods and techniques of eliciting admission and/or confession
	125. Guidance regarding proper taking, use and handling of investigative notes
	126. Concepts, principles, and practices of polygraph use
	127. Case-related information regarding government and private organizations’ functions and structure
	128. Concepts, principles, and practices associated with standard reporting format
	129. Agency-specific terminology, structure, instructions, correspondence procedures, or regulations
	130. Terminologies (including, but not limited to): • Medical/mental health terminology • Financial terminology • Legal terminology • Alcohol/Drug terminology • Criminal behavior terminology • Immigration and naturalization terminology
	131. Unique/precedent-setting case laws
	132. Computer and information systems usage guidelines
	133. Hostile countries and organizations
	134. Concepts and principles of clearance, access, reliability, suitability, and trustworthiness
	135. IT-based applications related to investigation (proper use, rules and guidelines)
	136. Concepts, principles, and practices of proper control of records